

Respecting Privacy While Conducting Investigations in Cyberspace

by

**David Gino Delaini
West Sacramento Police Department**

(May, 2011)

COMMAND COLLEGE CLASS (48)

The Command College Futures Study Project is a FUTURES study of a particular emerging issue of relevance to law enforcement. Its purpose is NOT to predict the future; rather, to project a variety of possible scenarios useful for strategic planning in anticipation of the emerging landscape facing policing organizations.

This journal article was created using the futures forecasting process of Command College and its outcomes. Defining the future differs from analyzing the past, because it has not yet happened. In this article, methodologies have been used to discern useful alternatives to enhance the success of planners and leaders in their response to a range of possible future environments.

Managing the future means influencing it—creating, constraining and adapting to emerging trends and events in a way that optimizes the opportunities and minimizes the threats of relevance to the profession.

The views and conclusions expressed in the Command College Futures Project and journal article are those of the author, and are not necessarily those of the CA Commission on Peace Officer Standards and Training (POST).

Respecting Privacy While Conducting Investigations in Cyberspace

Cyberspace has created a new canvas upon which the courts must determine what information should be protected under the Fourth Amendment to the United States Constitution. From self-publication on social networking sites to the increasing use of GPS based technologies in products being sold to consumers, the public is changing the manner in which they communicate and behave on almost an hourly basis. Despite the public's eagerness to broadcast their personal information in forums that are easily accessible by law enforcement professionals, they still insist they maintain a heightened expectation of privacy. The information posted on social networking sites and transmitted from GPS devices is often invaluable to law enforcement's ability to detect and solve crime. To avoid burdensome restrictions from the courts, though, it is imperative for leaders in the law enforcement community to guide the hands of their officers upon this canvas with an emphasis on responsible, ethical search and seizure practices.

Privacy Rights versus Privacy Practices

When asked, Americans state they not only want their "privacy rights" protected, they demand it (Boslet, Mixed signals on privacy concerns, 2008). The increasing frequency of self-publication by individuals on sites such as Facebook and Twitter have, no doubt, eroded expectations regarding how much privacy rights deserve to be protected. The dichotomy between the expectation and practice regarding personal privacy was well stated by Larry Ponemon, chairman of the Ponemon Institute (an independent privacy consultant), who said, "The vast majority of people want to protect their privacy, but they aren't doing anything about it" (Boslet, Mixed signals on privacy concerns, 2008). Indeed, two-thirds of people in developed areas, although purporting to be concerned about their privacy, are not so concerned that they

would want their information withheld if it made a particular online purchase more cumbersome (Boslet, Mixed signals on privacy concerns, 2008). A 2007 study conducted by the Pew Internet & American Life Project further highlights the profound difference between the expectation and practice regarding personal privacy. In that study, 94 percent of American adults surveyed said it was important to control who had access to their personal information. Sixty-one percent, however, had not taken any steps to limit the information about them found online (Boslet, Mixed signals on privacy concerns, 2008).

Attitudes regarding an individual's desire to protect his privacy online appear to cross generational lines. The Pew study found that almost an identical percentage of people in the 18 to 29 age group and the 50 to 64 age group say it is "important to control access to personal information" (Boslet, Internet users give mixed signals about online privacy concerns, 2008). In the same study, researchers found that 64 percent of people between the ages of 30 to 64 (as opposed to only 47 percent of people aged 18 to 29) had refused to give information to a business or company because they thought it was unnecessary or too personal (Boslet, Internet users give mixed signals about online privacy concerns, 2008). This disparity indicates the younger demographic is more open or reckless regarding the sharing of their information than they may realize.

The conflict between the public's expectation of privacy and practice regarding personal privacy has become even further exacerbated when examined in relation to law enforcement's access to information since September 11, 2001. According to House Judiciary Committee Chairman John Conyers (D-Michigan), "Americans are concerned with bad actors doing bad things, and if you ask them if they are comfortable with law enforcement checking (online data) related to people who, for example, are going to hurt children, by and large they are" (Sullivan,

RED TAPE CHRONICLES , 2010). Recent research indicates that some “69 percent of online Americans use at least one cloud based service, such as Web-based e-mail, and 64 percent of them said they were concerned law enforcement agencies could access their files” (Sullivan, RED TAPE CHRONICLES, 2010). Although these same people are not comfortable with the government having unfettered access to data, Conyers noted “the way people think about privacy is very context sensitive” (Sullivan, RED TAPE CHRONICLES , 2010). All the while, as the public’s opinions and practices regarding personal privacy evolve, the amount of data available to the law enforcement community continues to accumulate in cyberspace at a record pace.

To Connect and Share

Consumers jump at the opportunity to purchase new technologies, such as tablet computers, as quickly as those new technologies roll off the assembly line (Graham, 2010). Consumers are not just flicking on the power switch in isolation. As of September of 2009, 93 percent of teenagers and, as of December of 2009, 74 percent of adults, in the United States have utilized the internet (Amanda Lenhart, 2010). Of these connected individuals, 73 percent of teenagers and 47 percent of adults identified themselves as users of online social networking sites (Amanda Lenhart, 2010). Consumers are connecting and sharing information about their wants, needs, desires, thoughts, and even physical location with a level of openness on social networking sites, such as Facebook and Twitter. While using these technologies, consumers are leaving behind retrievable data that could be extremely valuable to the law enforcement community. As one author put it, “When you browse the Web, it's like you've allowed a bunch of companies to implant a tracking device in your arm and a small camera in your head, recording where you go and what you look at.” (Mogull, 2011). Notably, this extremely

valuable information is only a small part of the electronic information available to law enforcement.

More devices, including cellular telephones and cars, are being sold with GPS technology as a standard feature. When the public uses these GPS-enabled devices, service providers are collecting electronic data and may store the information for six months or longer, in part, to assist investigators (Cohen, 2011). Although the exact number of times an individual cellular telephone user's location is tracked may vary, in one case, an individual learned through legal action that, during a six month period, his cellular telephone service had recorded and saved his longitude and latitude coordinates more than 35,000 times (Cohen, 2011). This kind of electronic data may prove valuable to the law enforcement community. The mere knowledge that such data exists, though, provides little advantage to an investigator who cannot use the information in later legal proceedings because it was not collected in accordance with Fourth Amendment principles.

Online Privacy and the Law

The law enforcement community must understand not only how the public utilizes social networking sites and other technologies, but must also learn how to navigate this area of search and seizure. Unfortunately, this area of law is still evolving. These waters are relatively uncharted, though many of the basic principles have been established. Relating the core principals to new and unique factual circumstances will prove to be challenging. For example, as the case of People v. Diaz discussed below demonstrates, data stored on a cellular telephone may not receive the same protection that the same information stored on a compact disk would receive. The different privacy protection depends upon how the courts will apply past rulings to modern technologies not necessarily considered when the case establishing the rule was decided.

In another case, United States v. Pineda-Moreno, investigators analogized the use of a GPS tracking device to following a suspect in police vehicles (U.S. v. Pineda-Moreno, 2010). The United States Court of Appeals for the Ninth Circuit held that law enforcement may attach GPS devices to vehicles to monitor the movements of individuals in areas open to the public without the need for a court order (U.S. v. Pineda-Moreno, 2010). The Ninth Circuit reasoned that, if an officer may follow an individual on a public road by following him in a car or airplane, the use of greater technological advances to enhance that ability should not change the rule. Many law enforcement professionals found the Ninth Circuit's decision in United States v. Pineda-Moreno to be logical and expected.

On the other hand, a decision by the California Supreme Court, favorable to law enforcement's ability to exploit new technologies, took many by surprise. In People v. Diaz, the court held that an arresting officer may search a cellular telephone in the possession an individual incident to a lawful arrest, regardless of whether additional information beyond the naked arrest was present to support the intrusion (People v. Diaz, 2011). The decision was somewhat surprising because the United States Supreme Court's 2009 decision in Arizona v. Gant changed the way in which officers had been operating for over 30 years by establishing that officers could no longer search, incident to arrest, the vehicle an arrestee had been occupying just before his arrest (Arizona v. Gant, 2009).

In examining United States v. Pineda-Moreno and People v. Diaz, some law enforcement professionals question how the courts could allow an officer to unlock and search a cellular telephone incident to a lawful arrest when the officer could not look under the driver's seat of a vehicle from which that same suspect had recently alighted. The search restriction imposed by the court in Gant appears to have been based on a determination that something more than the

investigating officer's statement of "because the law says we can do it" (Arizona v. Gant, 2009) is necessary to support the search. To the interested onlooker, there does not appear to be any more justification than that to support the court's ruling in Diaz.

These cases demonstrate different approaches utilized by the courts to determine whether an individual had a reasonable expectation of privacy based on how the information or evidence seized was actually housed. A major factor in how this area of search and seizure law will be developed lies in the hands of law enforcement officers and the manner in which they pursue offenders.

On the Streets

Frequently, changes in the search and seizure laws do not occur contemporaneously with society's use of new technologies. Rather, the changes stem from active controversies; they arise when law enforcement officers have already taken some course of action. Accordingly, officers and deputies must look to past decisions to determine how they may seize the plethora of information available to them on social networking sites and GPS devices. Although the courts and legislature may not have defined what aspects of a technology-based search are private, those branches of government have established general privacy standards investigators must analogize to the circumstances of their case.

The analysis to be undertaken by law enforcement must focus on the standard; that is, whether a reasonable expectation of privacy is afforded to the individual from whom the information is being derived. By performing investigations in an ethical manner, and by emphasizing respect for the established privacy rights of individuals, the police have the ability to profoundly impact whether the courts will place burdensome restrictions on law enforcement efforts to mine this electronic data. In a time of challenged budgets and dwindling law

enforcement resources, reasonable accesses to this information can be of critical importance to the law enforcement community. This calls for action to ensure information readily available is not precluded from collection and inspection in the course of a criminal investigation.

As a result, law enforcement agencies throughout the nation should consider a two-prong approach regarding the search and seizure of data from social networking sites, GPS devices, and other modern technologies. First, they should provide officers with frequent training concerning modern technologies so officers and investigators can begin to understand and appreciate the vast amount of information available to them. The training should include information about the technologies, what the particular device or site can perform, how the public uses these technologies, and what type of information may be found by searching them. Second, and of equal importance, law enforcement managers must stay abreast of changes in search and seizure laws and develop in their officers the analytical skills necessary to analogize the particular facts of their case to the established search and seizure principles.

Conclusion

Those who are familiar with American jurisprudence know, “bad facts make bad law”. When the courts review search and seizure questions in areas that are not already well-settled, judges pay attention to what motivated the law enforcement officer to conduct a particular search. In examining these decisions, a trend becomes clear: where officers engage in misconduct or poorly and lazily perform their duties, the courts will place additional restrictions on law enforcement’s ability to search. One can readily see how a cavalier approach by law enforcement officials related to the mining of electronic data could have a significantly negative result regarding the level of efficiency with which criminals can be pursued. Consequently, properly oriented and ethically balanced officers play a critical role because, if law enforcement

managers can focus the development of investigators analytical skills in an ethical vein, the law enforcement community is far more likely to see less restrictive rulings from the courts. This is likely to hold true even when those of us in law enforcement, according to the judgment of the courts, get it wrong.

Bibliography

Amanda Lenhart, K. P. (2010, February 3). *Part 1: Internet adoption and trends, Who's online*. Retrieved March 1, 2011, from Pew Internet : <http://www.pewinternet.org/Reports/2010/Social-Media-and-Young-Adults/Part-1/Demographics.aspx>

Arizona v. Gant, 129 S. Ct. 1710 (SUPREME COURT OF THE UNITED STATES April 21, 2009).

Boslet, M. (2008, March 10). Internet users give mixed signals about online privacy concerns. *Inside Bay Area* .

Boslet, M. (2008, February 28). Mixed signals on privacy concerns. *San Jose Mercury News* .

Cohen, N. (2011, March 26). *It's Tracking Your Every Move and You May Not Even Know*. Retrieved March 29, 2011, from New York Times: <http://www.nytimes.com/2011/03/26/business/media/26privacy.html>

Graham, J. (2010, December 29). *Sales of tablet computers such as iPad outshine netbooks*. Retrieved February 28, 2011, from www.usatoday.com: http://www.usatoday.com/tech/products/2010-12-28-netbooks-predictions_N.htm

Grant, J. K. (2002). Ethics and Law Enforcement . *FBI Law Enforcement Bulletin* , 71 (12), 12.

Mogull, R. (2011, March 21). *Protect Your Privacy: Browse the Web Safely*. Retrieved March 29, 2011, from PC World: http://www.pcworld.com/businesscenter/article/222731/protect_your_privacy_browse_the_web_safely.html

People v. Diaz, 51 Cal. 4th 84 (California Supreme Court January 3, 2011).

Sullivan, B. (2010, April 13). *RED TAPE CHRONICLES* . Retrieved May 7, 2010, from MSNBC: <http://redtape.msnbc.com/2010/04/the-constitutional-issues-raised-by-cloud-computing.html>

U.S. v. Pineda-Moreno, 591 F.3d 1212 (UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT January 11, 2010).