



# 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.<sup>1</sup> 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.<sup>2</sup>

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.<sup>3</sup> 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.<sup>4</sup> There are today, for example, relatively expansive constitutional, statutory, and common law protections against government wiretapping and eavesdropping.<sup>5</sup> 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.<sup>6</sup>

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-

<sup>1</sup> 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).

<sup>2</sup> See, *Roe v. Wade*, 410 U.S. 113 (1973)

<sup>3</sup> 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).

<sup>4</sup> See, *Katz v. U.S.*, 389 U.S. 347 (1967).

<sup>5</sup> 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).

<sup>6</sup> 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.<sup>7</sup> 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.<sup>8</sup> 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.<sup>9</sup> Other citizen and consumer information privacy statutes, including the Privacy Act of 1974<sup>10</sup> and the Family Educational Right and Privacy Act,<sup>11</sup> soon followed. More recently, the Congress has enacted important protections for health records and financial records.<sup>12</sup>

## FAIR INFORMATION PRACTICE PRINCIPLES

In the early 1970s, two important studies developed the concept of “Fair Information Practice Principles” (“FIP Principles”).<sup>13</sup> 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.<sup>14</sup>

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

<sup>8</sup> See, *Whalen v. Roe*, 429 U.S. 589 (1977).

<sup>9</sup> 15 U.S.C. 1681 et seq.

<sup>10</sup> 5 U.S.C. 552a et seq.

<sup>11</sup> 20 U.S.C. 1232g; 34 CFR Part 99.

<sup>12</sup> 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>.

<sup>13</sup> 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>.

<sup>14</sup> 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.<sup>15</sup> 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.<sup>16</sup> The public is especially worried that their personal information will be captured and misused for identity theft—America’s fastest-growing crime.<sup>17</sup> 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.<sup>18</sup>

Privacy concerns are especially high when it comes to the Internet—the public commonly complains about a “sense of being watched” on the web.<sup>19</sup> 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,<sup>20</sup> and an equal number have refused to make an online purchase because of concerns about privacy or identity theft.<sup>21</sup>

## 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.<sup>22</sup> 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

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

<sup>16</sup> 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>).

<sup>17</sup> According to the Federal Trade Commission. See, [www.ftc.gov](http://www.ftc.gov) and [www.consumer.gov/idtheft/](http://www.consumer.gov/idtheft/).

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

<sup>19</sup> 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>.

<sup>20</sup> 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>.

<sup>21</sup> Cyber Security Industry Alliance poll, April 20-27, 2006. Available online at [https://www.csalliance.org/publications/surveys\\_and\\_polls/dci\\_survey\\_May2006](https://www.csalliance.org/publications/surveys_and_polls/dci_survey_May2006).

<sup>22</sup> *Supra*, note 18, at 5.

used and what type of offender is at issue (minors, violent offenders, etc.).<sup>23</sup> 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.<sup>24</sup> 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.<sup>25</sup> Eighty-five percent also agree that an individual ought to be notified when his criminal history records are accessed by a third party.<sup>26</sup>

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.<sup>27</sup> 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.<sup>28</sup>

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).<sup>29</sup> Each year, about 654,000 people are released from jail, prison or other incarceration.<sup>30</sup> 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.<sup>31</sup>

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.<sup>32</sup>

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-

<sup>23</sup> *Id.*

<sup>24</sup> *Supra*, note 14.

<sup>25</sup> *Supra*, note 18, at 5-6.

<sup>26</sup> *Id.* at 6.

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

<sup>28</sup> *Id.*

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

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

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

<sup>32</sup> 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.<sup>33</sup> Based, at least in part, on this research, most states have adopted standards for sealing and/or purging some or all aged conviction data.<sup>34</sup>

## 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.<sup>35</sup>

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.<sup>36</sup> 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.<sup>37</sup> 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.

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

<sup>34</sup> See, [www.removeit.org/eligibility](http://www.removeit.org/eligibility).

<sup>35</sup> *Supra*, note 18.

<sup>36</sup> *Id.*

<sup>37</sup> 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.<sup>38</sup>
- International sharing of criminal history information is expected to increase but also expected to be controversial.<sup>39</sup>
- 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 21<sup>st</sup> century is to balance public availability of criminal history record information with sufficient confidentiality protections to promote offender rehabilitation and reintegration.<sup>40</sup> 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."

<sup>38</sup> For a concise summary of these concerns, visit [http://www.epic.org/privacy/id\\_cards/](http://www.epic.org/privacy/id_cards/).

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

<sup>40</sup> 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](http://www.ncvc.org/ict).