It is good to catch crooks, murderers, and drug dealers. It is good to put them in jail, far from decent society, where, hopefully, they will redeem themselves.

Which is why there’s little or no fuss about the amazing and fast-expanding array of federal, state, and law-enforcement databases throughout the U.S. These little-known computer systems, governed and restricted by a patchwork of laws, hold enormous amounts of data about anyone who’s been arrested, anyone proven guilty of a misdemeanor, many victims of crime, and many witnesses and bystanders. The existence of, and the accuracy of, this crime-related data has a profound impact on law enforcement—it helps determine whether police can be granted a search warrant to search a suspect’s house, whether a prosecutor prosecutes or drops the case, and whether judges grant or deny bail.

But this storehouse of data, and the ease with which more is being collected, strikes many observers as creepy. Many others consider it an unwelcome expansion of police powers that unfairly entangle innocent people in investigations.

Some legal and ethical framework, Scharf argues, has to be developed to help police use the databases for good, while minimizing harm to citizens. This “is a sleeper issue for the Senate and the House,” which may have to deal with “a permanent digital underclass” of people whose legal criminal records of their crimes—petty or serious, repeated or solitary—are becoming widely available, costing these already disadvantaged people access to rental apartments, employment, and education, he said.

On March 14, 2002, the Wall Street Journal reported on the firing of Kimberly Kelly, a single mother employed as a pipe-insulator by a subcontractor to Eli Lilly and Co. Kelly lost her job not because of problems at work, but because heightened security concerns revealed she had bounced a $60 check in 2000, resulting in a misdemeanor conviction. She was one of 100 contract workers banned from Lilly’s sites. These 100 people are only a small part of a much larger trend, say some observers.
The number and scope of police networks and databases have increased in the last two decades. As of 2000, there were records for more than 59 million individual offenders in state criminal databases, according to a Department of Justice report, “Use and History of Criminal History Information: A Comprehensive Report, 2001 Update.” Roughly 85% of criminal intelligence data is stored by state and local forces, according to experts. There are somewhere between eight and 20 federal databases, including the Justice Department's National Crime Information Center (which stores criminal records and arrest warrants) and the Combined DNA Index System database (which keeps convicted felons' unique DNA “fingerprints”). Additional storehouses of data are kept by the Immigration and Naturalization Service, the Secret Service, and the Drug Enforcement Agency, among others.

Outside the beltway, the nation's 16,000-plus police jurisdictions also maintain a wide array of databases, which are increasingly linked with local government databases created by municipal courts, parole services, public defenders' offices, and the state Departments of Motor Vehicles (DMV). For example, the Automated Regional Justice Information System is used by 10,000 officials from 38 federal, state, and local agencies in San Diego County, Calif.

State and local databases are also melding into several regional networks. The Mid-Atlantic Great Lakes Organized Crime Law Enforcement Network (MAGLOCLEN) is headquartered in South- eastern Pennsylvania, and includes 470 agencies with over 162,761 sworn officers in federal, state, and local law enforcement, from Ontario to Maryland. MAGLOCLEN uses the federally funded Regional Information Sharing System, whose membership includes more than 304 state agencies and 685 federal agencies. Information about this array of databases can be found at www.it.ojp.gov.

There are also thousands of other databases that may yet be linked to these police networks. Security forces at universities, hospitals, and jails that keep their own databases, as do many private companies such as Wal-Mart, credit card agencies, and telephone companies. Many companies specialize in creating large-scale databases, which they now sell to advertisers, employers, lawyers, landlords, and increasingly hope to sell to private companies worried about crime and terrorism.

Much of this data never escapes from police computers. Data is hidden, lost or corrupted in flawed networks; cases can be closed without action; court records can be sealed; people connected to one crime may never be tangled up in another crime; and well-trained police can keep silent about the secrets they know. In a variety of inconsistent and incomplete fashions, state laws shield the identities of suspects, local regulations protect privacy, and federal laws curb unwarranted data collection.

Thus, the Electronic Communications Privacy Act sets tight rules for new wiretaps or for obtaining copies of a phone company's databases. A federal regulation, dating from 1979, and titled “28 CFR Part 23,” constrains data collection, and bars officials from browsing through existing data without a proper cause.

“I don't see any alarm or potential for problems,” says Pamela Scanlon, executive director of San Diego's Automated Regional Justice Information System. “We're pretty strict because it is important that you set an expectation at the beginning, through the career of an officer, about information and how it is used.”

But advocates for limiting police powers also see dangers.

Data collection technology is getting cheaper and easier—traffic cameras and face-recognition software, cell phones with precision-location gear, driver's licenses with digital data and biometric identification—while public suspicion is mollified by the promise of efficiencies and conveniences, and by the threat of terrorism. “The states...
are going hog-wild” in their efforts to collect new DNA data, complains Rachel King, the ACLU’s legislative counsel for criminal justice systems. For now, the ACLU has allied with right-of-center groups to oppose the growth of the databases, and especially the effort to create new high-tech driver’s licenses. But, she said, “at the national level, we’re having a hard time keeping our head above water since 9/11.”

State officials frequently try to limit the expanded use of the networks. For example, in Colorado, the traditional police line-up of suspects and innocents for inspection by witnesses is being extended to online line-ups, where witnesses review photographs supplied by special software at the state’s DMV. These online “perp walks” have elicited protest from Sen. Ron Teck, a Grand Junction Republican.

What is needed, says Scharf, is for the police networks to be separated by geography, purpose, sensitivity, and other factors, in order to help policymakers maximize the good and minimize the harm. For example, data about criminal gangs in one jurisdiction should be separated from other jurisdictions’ gang-related databases. Each jurisdiction’s databases should also separate gang-related activity from other criminal activities, Scharf said. Senior officials, judges, and legislators would then find it easier to write rules preventing unwarranted commingling of data that might unfairly implicate people with crimes, he said. Much of this segregation exists, but only because the newer technology—such as Google-type police browsers—is sporadically deployed. Existing state and federal laws provide some protections, but only in a patchwork fashion, he said.

Some data also needs to be kept hidden from the public when it enters the court system, argues Scharf’s colleague, Robert Stellingworth, the co-director of the Center for Society, Law, and Justice. Because most court reports are recorded on paper, they can’t be economically collected and sold by private companies, Stellingworth said. But courthouses are increasingly offering computerized records, allowing private firms to resell more people’s criminal records to prospective employers, landlords, and others. The result will be rape victims getting junk-mail pitches for “grief counseling,” he said.

These extreme examples, such as a rape victim being offered grief therapy, are relatively easy to prevent. But the most difficult problems reveal themselves in the mushy middle between what is obviously kept hidden (rape victims’ names) and what is obviously publicized (murderers’ names). For example, the 1979 regulations curb police from swapping data about people who are not suspects in a crime. But the distinction between a suspect, his or her partner-in-crime, neighbors, and family are frequently unclear, Stellingworth said.

The political terrain is made more complex by legislators’ priorities, said Scharf. Liberals are eager to collect information on people linked to spousal abuse and gun purchases, but conservatives are leery. In turn, conservatives are happy to have police gather data on likely terrorists, but they aren’t too troubled by the thought of employers and landlords learning more about their prospective employees and tenants.

Also, Scharf said, Republicans “may be more realistic than Democrats” about misuse of government data, following the still-mysterious release in the impeachment-for-perjury debate of embarrassing stories about then-Speaker Newt Gingrich, R-Ga., Rep. Bob Livingston, R-La., and Rep. Bob Barr, R-Ga.

No one has an easy answer to the step-by-step expansion of these networks. They can’t be effectively denounced as “Big Brother” because they’re simply too effective at the always-popular task of catching criminals, and occasionally, at proving innocent those already convicted.

“The unsatisfactory answer … is that we’ll have to wait and see,” said Orin Kerr, a former criminal division attorney at the U.S. Department of Justice, now teaching at George Washington University. But he is confident voters are aware of the trade-offs, and will push legislators to solve privacy problems when abuses are revealed. “I don’t see people missing the boat on privacy.”

Neil Munro (nmunro@njdc.com) covers the politics of the technology business for National Journal.