PRIVACY PROTECTION FOR DATA MINING SYSTEMS: TWO MODELS

Jeffrey Rosen

It is possible, in theory, to design any data mining system in ways that do a better or worse job at protecting privacy. Well designed systems could include systems of oversight that ensure that individuals are not linked with their data unless the system has identified them as especially dangerous. And controls could be placed on the sharing of information so that intelligence officials can only share with law enforcement officials evidence of serious crimes or terrorism, as opposed to low level crimes. I’ll call these two models of control the “traceable but not identifiable” model and the “control use” model.

For an example of the “traceable but not identifiable” model, consider the proposed Total Information Awareness program. The Defense Advanced Research Project Agency has studied technologies of “selective revelation,” which minimize personally identifiable information while allowing data mining and analysis on a grand scale. “The idea of selective revelation is that initially we reveal information to the analyst only in sanitized form, that is, in terms of statistics and categories that do not reveal (directly or indirectly) anyone’s private information,” writes a DARPA report called “Security With Privacy.” “If the analyst sees reason for concern he or she can follow up by seeking permission to get more precise information. This permission would be granted if the initial information provides sufficient cause to allow the revelation of more information, under appropriate legal and policy guidelines.”

The Total Information Awareness office had a project called Ginisys that explored ways of conducting general data searches where the data traceable but not easily identifiable – in other words generally anonymous unless officials receive permission to link the data with a particular individual. According to the program director, Ginisys could protect privacy by separating identifying information from the personal
transactions, only recreating the association when there is evidence and legal authority to do so. This might allow, for example, the Center for Disease Control to have access to medical information while other groups do not. The Ginisys staff also planned to develop information privacy filters to keep information that is not relevant out of the repository — encouraging the government to adopt laws that limit the types of data that can be recorded about specific people or transactions. Finally, Ginisys planned to use software agents to mine the information in the repository to expunge information that is unrelated to terrorism.

These are promising first steps toward the creation of an architecture of surveillance that might, in theory, protect privacy by imposing controls on how data is used; but it’s clear that privacy can’t be protected by technology alone. For the system to work, Congress would have to create a series of oversight mechanisms to ensure that the system is focusing on potential terrorists rather than innocent citizens. Congress could also create a special oversight court with the authority to decide when identifying data obtained during mass data surveillance may be connected to transactional information. After intelligence analysts have identified a series of transactions that they believe might be evidence of a terrorist plan, they could petition the special court for authorization to identify the individuals concerned. In considering whether to grant the request, Congress could direct the court to satisfy itself that the crime for which evidence has been presented is a serious threat of force or violence, and that the evidence suggests a link between the suspects and organized terrorists. If the court granted the order, the analysts could link the identifying information with the transaction data, and they could contact federal, state, and local law enforcement officials to inform them of the threat. In addition to creating this oversight body, and determining legal standards to guide its operation, Congress might also create standards for federal and citizen oversight, along with penalties for abuse; a dispute resolution process that would give citizens recourse when their data is incorrect or misused; and a series of fair information practices that would give citizens the right to know what personal information the government has collected and to correct any inaccuracies.

Merely to describe the complexity of these oversight mechanisms is to raise questions about their practicality. For this reason, controls on the sharing of information may be more effective than attempts to separate individuals from data. As a model for the “control use” model, consider the evolution of the new Computer Assisted Passenger Pre-Screening system, called CAPPS II, which is now being tested and which the administration plans to put in place later this year. Initially, the CAPPS II program contemplated data mining along the Total Information Awareness model; but in response to criticism, it now will be limited to the goal of “authenticating” airline passenger information, not searching for profiles of terrorist activities. Authenticated names will ideally be matched against watch lists of known terrorist suspects (and it is important that these watch lists not expand to include all suspects of lower level crimes.) Under the current version of the program, each passenger’s name, address, home phone number and date of birth will be linked to two commercial databases, Lexis-Nexis and Axiom, which collect information about consumer habits. The data may not contain medical or bank-account information, but may include information about passengers’ magazine subscriptions and buying patterns, where family members live, and how long they have owned a car. Based on the information, passengers will be assigned to green, yellow or red categories, and will be subject to corresponding scrutiny.

In its initial announcement last January, the administration proposed to share personal data from the CAPPS II system with national and international police to allow the prosecution of any civil or criminal violations. But critics objected that this could create widespread abuses, allowing the administration to scour the personal data of millions of people, uncover relatively minor offenses, and threaten its critics with vindictive prosecutions — much as Richard M. Nixon scored the tax returns of Vietnam protesters. In response to these criticisms, the Transportation Security Agency agreed last August to restrict officials from sharing personal data with law enforcement agencies, except for individuals who had an outstanding federal warrant for a violent crime.

This was a welcome and important victory for privacy. Some additional checks and balances would help — people need a chance to correct their data, for example, and the system should be legally restricted to airports to ensure that citizens’ threat rankings don’t trail
them in all of their interactions with the government. But the attempt to limit the search for data and sharing of personal information — so that the system is focused on the most dangerous suspects and criminals rather than on trivial offenses — could be a model for the rest of the federal government.

The two models I’ve identified could guide efforts to reform the Patriot Act. Federal officials have already invoked the Act’s surveillance authority to prosecute citizens and noncitizens for low-level crimes that have nothing to do with terrorism. In addition, the Act allows the government to conduct secret searches of information held by third parties without notice to the individual involved. In theory, then, the government could secretly scour the personal data of its critics and use the information to embarrass or prosecute them.

But there is a sensible way that this danger could be eliminated. In the Senate, a bipartisan coalition including Larry Craig, Republican of Idaho, and Richard Durbin, the Illinois Democrat, have introduced a bill called the SAFE Act that would allow for the Patriot Act’s secret searches of personal information held by third parties, but only when an individual has already been identified as a suspected spy or terrorist. This is a version of the “traceable but not identifiable” model — it allows individuals to be linked to their data only after they have been identified as suspicious.

The problem with the SAFE Act is that it might make it harder for intelligence officials to pursue leads about suspicious individuals who may appear dangerous, but not enough to be immediately identifiable as suspected terrorists. For this reason, the Patriot Act might also (or instead) be reformed with a version of the “control use” model. In Germany, which over the last 60 years has learned all too well the dangers of too-powerful security services, the intelligence service is given broad powers of domestic surveillance, but if officers find evidence of low-level crimes, they may not share it with law enforcement officers or introduce it in court. In addition, evidence obtained through wiretapping can be used only in the investigation and prosecution of national security crimes or certain other serious crimes.

The compromises that I’ve described – the control use model, which limits the circumstances under which data can be shared and the particularized suspicion model that ensures that only suspected dangerous individuals are linked with their data – could help to ensure that data mining systems protect privacy. Whether they are an effective way of increasing security is an entirely separate question.