Op-Ed When it comes to protecting its citizens' data, Europe is way ahead of the U.S.

By JAMES B. RULE

MAY 12, 2014, 6:54 PM

Americans haven't had much good news about their privacy since Edward Snowden launched his soap opera of NSA revelations last June. True, the president, Sen. Diann Feinstein and Patriot Act co-author Rep. Jim Sensenbrenner are finally distancing themselves from the most outrageous snooping. But it hasn't stopped. According to the New York Times, a request from one U.S. phone company to cease sharing its records with the National Security Agency was rebuffed in March by the Foreign Intelligence Surveillance Court — the secret federal tribunal that mostly seems to specialize in saying "yes" to surveillance.

About half of Americans tell pollsters they are alarmed by these trends. Others appear resigned to a pervasive loss of privacy as the inevitable cost of life in an information society. But there is no reason to draw such a dire conclusion. Technology can hardly rob us of our privacy unless bidden to do so by political and legal imperatives.

Europe, another information society, does much better at defending its citizens' privacy. At about the same time the FISA court was upholding NSA claims on Americans' telecommunications data, the European Court of Justice in Luxembourg ruled to precisely the opposite effect. It struck down laws mandating long-term retention of consumers' telecommunications data. National legislation requiring retention of such records (and hence, their availability for state scrutiny) for up to two years will have to be rewritten. In strong language, the court cited the lack of adequate safeguards "against the risk of abuse and against any unlawful access and use of the data" as a threat "to respect for private life and to the protection of personal data."

Why don't we find American courts issuing such sweeping defenses of privacy? Much of the explanation surely lies in the contrasting legal strategies and principles adopted by this country and by Europe. Europe has created rights applying to government and private-sector treatment of personal data in general, across different institutions and contexts of use.

These broad privacy rights were established in a directive adopted by the European Parliament and the Council of the European Union in 1995 and are now being updated. Like other such directives, on matters ranging from antitrust law to copyright, the 1995 privacy directive requires that all 28 EU countries "transpose" — i.e., incorporate — its principles into their national legal codes.

Among other things, the privacy directive prohibits "secondary" release of personal information. This is the sharing of such data for purposes other than those for which they are originally provided — in

the course of retail sales, for example, or medical care delivery or charitable giving. To waive this prohibition, Europeans must affirmatively grant permission for each subsequent reuse; otherwise, names, addresses and other personal information must remain with the organizations to which the data were originally provided.

One concrete result of this simple but potent principle is that Europeans' post boxes and electronic inboxes do not groan under the weight of unsolicited junk mail that Americans confront daily.

American privacy law, by contrast, establishes no such broad rights. Our most comprehensive such legislation, the Privacy Act of 1974, offers limited protections to certain categories of federally held personal data. Other national legislation is "sectoral" — applying different restrictions to personal data held in different settings, such as consumer credit or healthcare delivery. Thus, when new settings arise — say, social media or mobile communications — privacy activists must scramble to promote new safeguards, with no guarantee of success. As German computer law expert Wolfgang Kilian puts it, compared with EU privacy law, "the U.S. system looks more like, 'everything is allowed unless it is forbidden.'"

The European approach is stronger. When new uses of personal data are contemplated, it's known in advance that they must conform to established privacy rights, a major deterrent to privacy-unfriendly interests. Of course, both strong legal structures and serious political will are necessary to make these rights real in practice. But at this stage, Europe leads the United States in both departments.

Could the U.S. establish European-style rights over personal information? There's no reason why not — other than the low level of concern for privacy among this country's political elites.

A number of American privacy advocates, for example, have proposed creating some form of residual right over commercial reuse of personal data so that data provided in one setting (online sales, for example, or website visits) could not be sold or traded for further use without permission. Such new rights would resemble an author's copyright over her work, or a property right over commercial exploitation of personal data or a fiduciary obligation binding on parties entrusted with such data.

Celebrities already enjoy rights something like this over the commercial use of their names and images. No one may open a restaurant named after a sports hero or movie star without permission from (and, normally, compensation to) that athlete or actor.

Drafting legislation extending such rights to ordinary citizens would hardly be complicated. But the political forces that would rise in opposition are daunting. Too many industries and government agencies in this country flourish by appropriating personal information without permission from, or even the awareness of, those concerned.

Yet the European example shows that restrictions on such practices are hardly incompatible with a vibrant information society. Google and Facebook, for example, have both recently accepted privacy restrictions imposed by European courts, without evident damage to their bottom lines.

The European model is feasible. But only if ordinary Americans grasp that dramatic alternatives exist to current, privacy-eroding practices, and demand strong, comprehensive privacy rights.

James B. Rule, a researcher at the Center for the Study of Law and Society at UC Berkeley, is the author of "Privacy in Peril: How we are Sacrificing a Fundamental Right in Exchange for Security and Convenience."