February 4, 2012

Should Personal Data Be Personal?

By SOMINI SENGUPTA

MAX SCHREMS, a 24-year-old law student from Salzburg, Austria, wanted to know what Facebook knew: He requested his own Facebook file. What he got turned out to be a virtual bildungsroman, 1,222 pages long. It contained wall posts he had deleted, old messages that revealed a friend's troubled state of mind, even information that he didn't enter himself about his physical whereabouts.

Mr. Schrems was intrigued and somewhat rattled. He wasn't worried about anything in particular. Rather, he felt a vague disquiet about what Facebook could do with all that information about him in the future. Why was it there at all, he wondered, when he had deleted it? "It's like a camera hanging over your bed while you're having sex. It just doesn't feel good," is how he finally put it. "We in Europe are oftentimes frightened of what might happen some day."

Mr. Schrems's sentiment is emblematic of the discomfort sweeping through Europe about the ways in which Internet companies treat personal information. That discomfort has, in turn, prompted proposals for stricter regulation of online data across the continent. And Europe's moves to protect Internet privacy — something Americans have not, as yet, actively agitated for — have given rise to a thorny question: How do the laws and mores of different nations manage, if at all, the multinational companies that now govern our digital lives?

Personal data is the oil that greases the Internet. Each one of us sits on our own vast reserves. The data that we share every day — names, addresses, pictures, even our precise locations as measured by the geo-location sensor embedded in Internet-enabled smartphones — helps companies target advertising based not only on demographics but also on the personal opinions and desires we post

online. Those advertising revenues, in turn, make hundreds of millions of dollars for companies like Facebook, which announced last week that it was going public in what is expected to be the largest I.P.O. in digital history. And those revenues help to keep the Web free of charge.

But there is a price: that data about our lives and wants are collected, scrutinized and retained, often for a long time, by a great many technology companies. Personal data is valuable. In the United States alone, companies spend up to $2 billion a year to collect that information, according to a recent report from Forrester Research.

The European media seized on Mr. Schrems's discovery. German newspapers published instructions on how to request personal data files from Facebook. Within a few months, 40,000 people had made similar requests. The data protection office in Ireland, where Facebook has its European data center, conducted an audit of Facebook's data retention practices; the company agreed to overhaul the way it collects data in Europe, including disposing of user data "much sooner." German regulators have scrutinized facial recognition technology. The Netherlands is considering a bill that would require Internet users to consent to being tracked as they travel from Web site to Web site. And last month, the European Commission unveiled a sweeping new privacy law that would require Web companies to obtain explicit consent before using personal information, inform regulators and users in the event of a data breach and, most radical, empower a citizen of Europe to demand that his or her data be deleted forever.

"Europe has come to the conclusion that none of the companies can be trusted," said Simon Davies, the director of the London-based nonprofit Privacy International. "The European Commission is responding to public demand. There is a growing mood of despondency about the privacy issue."

Every European country has a privacy law, as do Canada, Australia and many Latin American countries. The United States remains a holdout: We have separate laws that protect our health records and financial information, and even one that keeps private what movies we rent. But there is no law that spells out the control and use of online data.

It would be tempting to say that history and culture on this side of the Atlantic make privacy a non-issue. That's not exactly the case. Privacy has always mattered

in American law and to American sensibilities, but in a different way.

Anxieties over privacy came up when postcards were first sent in the late 19th century. The advent of photography prompted Samuel Warren and Louis Brandeis, in an 1890 article in The Harvard Law Review, to warn of the dangers of displaying private family wedding pictures in the pages of every newspaper. And in one of the most important privacy decisions in recent years, the Supreme Court in January ruled that police officers violated the Constitution when they placed a Global Positioning System tracking device on a suspect's car, to monitor its movements. "Europeans are much more sensitive about controlling their image online," said James Q. Whitman, a Yale Law School professor who has written about the differences in jurisprudence between the United States and Europe.

Social mores around privacy vary widely across the globe. In Japan, Google was criticized for being intrusive when its self-driven cars cruised the streets with a camera snapping pictures for Google Street View.

In India, where I was a correspondent for this newspaper for more than four years, the notion of privacy seems foreign. A shopkeeper might casually ask a childless woman if she has gynecological trouble; school grades are posted on public walls; many people still live in extended families, literally wandering in and out of one another's bedrooms. But a project to issue biometric identity cards to every Indian citizen recently set off a flurry of concern over privacy, prompting the government to draft a new law that enshrines the right to privacy for the first time.

IN the United States, federal legislation on online privacy has languished, as lawmakers weigh the interests of consumers and companies in the battle for personal information.

Part of the difficulty in regulating online privacy is the speed of technological innovation. Just as it becomes remarkably easy for us to share our information with others, it also becomes cheaper and easier to crunch and analyze that information — and store it forever, if necessary.

Stewart A. Baker, a former assistant secretary at the Department of Homeland Security, is among those who see enormous benefits for private companies and government agencies alike. To fight it on privacy grounds, he argued, would be

largely futile. “You can’t really have a property interest in data,” he argued. “It’s going to get cheaper to reproduce it. It’s going to get reproduced and stored. It’s going to get copied.”

Privacy advocates worry about the consequences. Most people may not have much to hide. For a few, not sharing personal information may be vital. They’re the ones who need the protection of the law, argued Rebecca MacKinnon, a fellow at the New America Foundation and author of “Consent of the Networked,” a book about digital freedom.

“It may be victims of domestic abuse who don’t want to be stalked or tracked, or it could be dissidents in Syria, or someone who has weird opinions and could mistakenly end up on a watch list when they don’t deserve it,” said Ms. MacKinnon. “If you have a democratic society, the point is not to say whatever is good for the majority is all we need.”

Somini Sengupta is a technology reporter for The New York Times.