Privacy Lost: EU, U.S. laws differ greatly

EU citizens well protected against corporate intrusion, but red tape is thick

B
T
updated 10:19 a.m. CT, Thurs., Oct. 19, 2006

It started, some say, with Alexandre Dumas, famed French author of “The Three Musketeers.”

Dumas was an aging French literary star when he embarked on a somewhat scandalous love affair with Adah Isaacs Menken, a 32-year-old Texas actress. Enranced with the still-young technology of photography, the two posed for clearly scandalous photographs. The photographer, smelling a quick profit, set out to sell them, and Dumas sued.

A Paris appeals court quashed this early paparazzi moment. In a ruling that sounds quaint to the modern American ear, the court decided that posing for the photographs did not mean Dumas and Menken had surrendered their rights to privacy and dignity, even if they consented to do just that during a heady romantic moment. These rights trumped any commercial property rights the photographer might have claimed, the court said.

“One sale by a person who had momentarily ‘forgotten his dignity’ had to remain effectively voidable.” Yale law professor James Whitman wrote of the ruling in a paper titled “The Two Western Cultures of Privacy: Dignity versus Liberty.” “One’s privacy, like other aspects of one’s honor, was not a market commodity that could simply be definitively sold.”

European courts and lawmakers have been wrestling with the implications of technology and privacy ever since, often coming to conclusions that are foreign to their American counterparts.

In Europe, privacy is different

Some of those rulings might seem like a panacea for Americans who believe their privacy is slowly slipping away

In many parts of Europe, for example:

- Personal information cannot be collected without consumers’ permission, and they have the right to review the data and correct inaccuracies.
- Companies that process data must register their activities with the government.
- Employers cannot read workers’ private e-mail.
- Personal information cannot be shared by companies or across borders without express permission from the data subject.
- Checkout clerks cannot ask for shoppers’ phone numbers.

Those rights, and many others, stem from The European Union Directive on Data Protection of 1995, which mandated that each EU nation pass a national privacy law and create a Data Protection Authority to protect citizens’ privacy and investigate attacks on it.

National laws come in several flavors, and emanate from varied traditions. But taken together, they are the backbone of a basic European principle: Privacy is a human right.

In this clear declaration, Europe ventures far from the patchwork approach taken by U.S. lawmakers. But a privacy heaven, it’s not.

European trust government more

With those privacy protections come other, curious laws and regulations that would fluster most Americans.

Authorities in some European countries can veto a parent’s choice for their baby’s name in the name of preserving dignity, for example. Government officials also often cloak themselves in dignity to limit freedom of the press and evade public scrutiny.

Most important, while companies face severe regulations limiting their use of consumers’ personal information, governments are largely exempt from such limitations. While the use of credit reports is rare in Europe, wiretapping is
not. In the Netherlands, for example, wiretaps are 130 times more common than in the U.S. Many Europeans carry some kind of national ID card, still unthinkable for many in the U.S. In Germany, every citizen and long-term visitor must register his or her address with the police.

The reason that privacy laws in Europe and the U.S. are so different springs from a basic divergence in attitude: Europeans reserve their deepest distrust for corporations, while Americans are far more concerned about their government invading their privacy.

As a result, U.S. federal agencies have been given little power to limit the potentially privacy-invading behaviors of private companies. The Federal Trade Commission, the agency charged with protecting U.S. citizens from such intrusions, rarely acts against U.S. firms. When it does, its remedies are generally limited to small fines and out-of-court settlements.

Each European nation, on the other hand, has its Data Protection Authority to monitor corporate behavior. Consumers can appeal to the authority, which in some countries boasts far-ranging subpoena power. Fines for misbehavior are common.

**Legacy of the Holocaust?**

Some privacy experts argue that heightened European sensitivity to privacy stems from the horror of the Holocaust, when the Nazis used public and church records to identify Jews to be rounded up and sent to concentration camps. But others say the historical difference dates back much further – to Dumas, or even earlier, and the notion that governments are charged with actively protecting people.

“In Europe the first line of defense against private wrongdoing is the state,” said Joel R. Reidenberg, privacy expert at Fordham University School Law School. “In the U.S. our instinct is more liberal: Let private actors sue each other.”

These differences are more than theoretical, and several times have threatened to trigger trade and culture wars:

- A post-Sept. 11 data sharing agreement that provided U.S. authorities with 34 pieces of information on each airline passenger entering the country on flights from Europe was ruled illegal earlier this year by the European Supreme Court. The dispute threatened to ground all flights into the U.S. from Europe until the U.S. Department of Homeland Security and the European Union announced a settlement on Oct. 6.
- In June, the New York Times revealed that U.S. anti-terrorism officials are mining data from the Belgium-based Society for Worldwide Interbank Financial Telecommunications (SWIFT), which regulates most international banking transactions. Belgian officials opened an immediate investigation. Such data mining would be considered illegal under Belgian law.
- In the late 1990s, e-commerce between Europe and the U.S. almost came to a halt after the EU’s Data Protection Directive barred transfer of data to countries without comprehensive privacy protection laws. By EU standards, the U.S. falls far short of the requirements. Two years of negotiations ended in a “safe harbor” agreement promising privacy controls on EU data that flows into the U.S. Complaints about the system persist, however, from both sides.

**Market efficiency vs. dignity**

U.S. firms criticize the European limitations on data gathering, saying that regulations enforcing them are cumbersome and put Europe at a competitive disadvantage.

For example, only debtors who’ve defaulted on loans generally receive the European equivalent of a credit report, which places them on a sort of lending blacklist. Consumers who pay their bills on time do not get a “good” credit score.

Critics say that’s a disadvantage because credit reports make consumer lending much safer for lenders, thereby reducing the cost of credit and increasing consumers’ ability to borrow.

But defenders of the European system point to places like the U.K. and Ireland, where there’s little evidence that access to mortgage loans is limited.

But there is a larger notion at stake than availability of credit. In Europe, the laws tend to protect consumers from unnecessary public humiliation at the hands of corporations.

“The basic issue is … not just one of market efficiency. Consumers need more than credit. They need dignity,” writes Whitman, explaining the prevailing European thought. “The idea that any random merchant might have access to the ‘image’ of your financial history is simply too intuitively distasteful to people brought up in the Continental world.”
In U.S., home is where the privacy is
In stark contrast, U.S. privacy is squarely equated with liberty from a prying government.

The word privacy does not appear in the Constitution, but it is has been constructed by legal scholars using elements of the Bill of Rights, such as the Fourth Amendment—which bans unreasonable search and seizure. U.S. residents cherish the right to be left alone in their homes, and courts have generally been supportive of this right. However, once a person leaves the home — physically or virtually — the right to privacy quickly dissipates.

In much of Europe, allowing employers to read employee e-mails would be considered an attack on dignity — much like the publication of Dumas’ risqué photographs.

In October 2001, for instance a French court ruled that Nikon France could not fire an employee for performing freelance work on the job because the incriminating e-mails were marked “personal,” and thus could not be used as grounds for dismissal.

In the U.S., employees surrender most of their rights to privacy when they enter and use company property.

European and U.S. laws also diverge widely on limiting press freedoms, with U.S. courts granting wide leeway over publication, even of intimate photographs and personal details.

Whitman sites this dramatic distinction as an example:

In 1985, a gay man successfully sued a French publication to prevent publication of a photo of him at a gay pride parade in Paris. A few years earlier, the California Supreme Court upheld the right of journalists to identify San Francisco resident Oliver Sipple as a homosexual after Sipple helped foil an assassination attempt on then-President Gerald Ford. Sipple was declared a public figure by the court, and thus surrendered much of his privacy rights. The hero, who had hidden his sexual orientation from his Midwestern family, ultimately committed suicide.

Piecemeal approach vs. comprehensive law
Neat-and-clean comparisons between Europe and the United States aren’t always possible, however.

There are narrow laws that protect dignity in the U.S., such as the Video Privacy Protection Act, quickly passed in 1988 after a newspaper published the video rental records of Judge Robert Bork during his heated Supreme Court nomination hearings.

And often state legislatures have been aggressive in passing legislation protecting personal information.

California’s 2003 data breach notification law, which requires companies to tell consumers when there personal information has been lost or stolen, and similar laws subsequently enacted in other states are directly responsible for the public disclosure of dozens of data leaks and about 90 million consumer notifications.

To George Washington University professor Daniel Solove, that distinction is really the greatest difference between the privacy approaches in Europe and the U.S.

“U.S. law has arisen haphazardly, in reactive fashion,” Solove said. “The U.S. system is more fractured than other countries, so it’s harder to pass broad, all-encompassing legislation. There are so many industries with well-paid lobbyists ready to pounce, the minute you propose anything of any breadth you are inundated with whiny companies that come in and shout ‘Not me. not me.’ … It’s easier to do something pretty narrow and go after the ‘now’ problem and limit the amount of companies that are angry at you.”

It’s really 26 EU nations vs. 50 states
Talk of “European privacy law” also is a generalization. The European Privacy Directive is a guideline for EU nations, but each has its own national law and an agency that interprets that law. There are major variations from country to country, says Ashley Winton, an international privacy law expert in White & Case law firm’s London office.

“The directive talks about obtaining explicit consent from data subjects (before data is shared),” he said. “In Germany, they are very strict about what that means. They want a little bit of paper with real ink on it.” Other nations accept far simpler methods for consent, he said.

Winton’s White & Case counterpart in New York, international privacy lawyer David Bender, is skeptical of the EU approach, which he says hamstrings companies trying to do business in Europe with unmanageable red tape.
For example, can a U.S.-based cell phone user traveling in Europe talk to a customer service agent there without first giving written permission for a case to be entered in a database?

The regulations governing the passage of information from Europe to the U.S. are often so strict that many companies largely ignore them.

“In all my years of practice I have never heard clients come in and say, ‘OK, what do I have to do to be 70 percent compliant?’ I hear that now,” he said.

The bigger question, Bender argues, is whether the additional protections and regulations result in Europeans enjoying more privacy than Americans.

The answer is “no,” he said, pointing to a study this year by the Ponemon Institute that was commissioned by White & Case. The study found that U.S.-based multinational firms scored higher than their European counterparts on five of eight common privacy practices, including having a dedicated privacy officer and better computer data security.

**Privacy law: Not the product of logic**

Other privacy experts are skeptical of such measurements. After all, if privacy as a concept is hard to define, quantifying levels of privacy seems almost impossible.

“How do you assess whether there is a greater privacy protection or not (in Europe),” Solove said. “To what extent do people have rights? It’s hard to measure.”

Some U.S. privacy experts are less bashful in their support of Europe’s legal privacy framework. Marc Rotenberg at the Electronic Privacy Information Center and other privacy advocates regularly call for adoption of similar comprehensive U.S. privacy laws, including the right to challenge the accuracy of personal information companies hold.

But given the difficulty Congress has had passing any privacy-related legislation, it’s hard to imagine it will opt for an “all for one, one for all” approach with Europe any time soon.

Earlier this year, after it was reported that a blogger purchased presidential candidate Gen. Wesley Clarke’s cell phone records online for about $100, lawmakers churned out outraged press releases, held nearly a dozen hearings, convened an investigative panel and introduced several bills aimed at restricting the practice. None has been adopted.

While the debate was going on, investigators working for Hewlett-Packard were lying about their identities to obtain reporters’ phone records. And when that news finally broke, there were more hearings and extensive debate over whether or not the act of lying to get phone records was illegal. Again no action was taken.

As a result of such reluctance, people on both sides of the Atlantic are likely to live with two very different privacy regimes for some time. But perhaps that’s not surprising, given the disparate foundations from which they spring.

"Privacy law is not the product of logic,” Whitman reminds readers. “Nor for that matter is it the product of experience. It is the product of local social anxieties and local ideals.

“In the United States those anxieties and ideals focus principally on the police and other officials, and around the ambition to secure the blessings of liberty; while on the continent they focus on the ambition to guarantee everyone’s position in society, to guarantee everyone’s honor.”

© 2007 MSNBC Interactive

URL: http://www.msnbc.msn.com/id/15221111/

MSN Privacy . Legal
© 2008 MSNBC.com