THE WALL STREET JOURNAL.

http://www.wsj.com/articles/SB10001424127887324338604578328393797127094

JOURNAL REPORTS: LEADERSHIP

Should the U.S. Adopt European-Style Data-Privacy Protections?

March 10, 2013 4:00 p.m. ET

Companies are watching you. They want to know where you go on the Web, what you buy and what causes you support—with the hope of sending you targeted offers based on your preferences and lifestyle choices.

But who is watching over these businesses? Who is making sure they aren't misusing personal data or breaking privacy promises they make to customers?

In Europe, there are strict rules about what companies can and can't do in terms of collecting, using, disclosing and storing personal information, and governments are pushing to make the regulations even stronger. That has prompted renewed debate about whether it is time for the U.S. to toughen its relatively lax privacy regulations.

In one camp are those who believe the U.S. government should refrain from meddling. They say the lack of privacy restrictions in the U.S. has encouraged innovation in the online-marketing industry, which is still evolving, and they question whether a Congress that isn't capable of passing a budget can be trusted with crafting complex privacy legislation.

The U.S.'s experiment with self-regulation has been a failure, say those who believe Europe's approach to privacy is superior. By trusting industry to police itself, the U.S. has created a situation where consumers have little control over personal data and few remedies when they find their privacy has been invaded.

Yes: Our Experiment With Self-Regulation Has Failed

By Joel R. Reidenberg

JOURNAL REPORT

- Insights from The Experts (http://stream.wsj.com/story/experts-leadership/SS-2-135537/)
- Read more at WSJ.com/LeadershipReport (http://online.wsj.com/public/page/journal-report-leadership.html?mg=inert-wsj)

MORE IN UNLEASHING INNOVATION: BIG DATA

- How Big Data Is Changing the Whole Equation for Business (/articles/SB10001424127887324178904578340071261396666)
- Big Data, Big Blunders (/articles/SB10001424127887324196204578298381588348290)
- The New Shape of Big Data (/articles/SB10001424127887323452204578288264046780392)
- Moneyball, VC Style (/articles/SB10001424127887323384604578326221992355916)
- A Guide to Facebook's Privacy Options (/articles/SB10001424127887324880504578300312528424302)

VOTE

Thirty-five years ago, a federal commission studied privacy protections in the U.S. and concluded that "neither law nor technology now gives an individual the tools to protect his legitimate interests in the records organizations keep about him."

If that was the conclusion then, imagine what the commission would say about privacy today in the age of cloud computing and big data.

Sensitive health information gleaned from the websites we visit is collected and sold, GPS and cell-signal location tracking by the police is conducted without warrants, and online retailers target consumers for higher prices based on their Web browsing histories. Industry self-regulation and options like privacy settings on social networks, Web browsers and mobile apps have failed to keep up with advances in invasive tracking techniques. Our limited legal rights don't come close to protecting us against online tracking and profiling.

In contrast to the U.S., the European Union has a comprehensive set of legal rights to protect personal data. Every country in the EU has a statute establishing fair information practices for the collection, use, disclosure and storage of personal information, and has combined these rights with remedies for violations and the creation of an independent government agency for oversight. This European model has significant merits compared with the U.S. piecemeal approach.

Citizens come first. Europe's system recognizes that privacy, regardless of context, is a

Joel R. Reidenberg *DAVID WENTWORTH/FORDHAM LAW SCHOOL*

Tale of the Tape | Data Privacy in Europe

FUNDAMENTAL RIGHTS
European Union law explicitly enshrines privacy as a fundamental right. The European Convention on Human Rights, to which all EU nations are signed, says "everyone has the right to respect for his private and family life, his home and his correspondence." More-specific privacy regulations in Europe are grounded in this right.

THE LAWS
The EU has several "directives" that require member states to make laws regulating the collection, storage and use of personal information. The laws must prohibit companies from collecting and using data in many circumstances unless the individual gives permission. They also must allow people to see what data companies have about them and to demand correction or deletion of information.

INTERNET RULES
When it comes to privacy on the Internet, the EU recently began requiring countries to have rules that make websites get people's consent for the use of tracking technologies such as cookies, which are small files stored on people's computers. These laws are going into effect across Europe, but some specifics of compliance and enforcement are still unsettled.

COUNTRY BY COUNTRY
Some EU countries are stricter with their regulations than others. The Netherlands, for instance, says users must actively give their consent before websites can install cookies. The U.K., on the other hand, requires only a prominent notice that cookies are being used; if the person continues browsing, the site can assume that consent is implied. On another front, Spain is in a legal fight with Google after its Data Protection Agency ordered the search giant to remove links to information and news stories about private individuals.

REGULATORY POWERS
National data authorities in the EU have the ability to investigate companies and require them to delete stored information or pay fines. Companies can contest the regulators by taking the matter to court. Individuals can also bring complaints based on the laws.

—*Jennifer Valentino-DeVries*

core democratic value that must be safeguarded, not left to market forces. In the U.S., companies reveal only what they want about their data practices, privacy notices are largely incomprehensible and companies can rewrite their policies after collecting your data.

One size doesn't fit all, though, and the rigid implementation of privacy laws can bring unintended consequences—like a ban on hidden filming that would treat the taping of police behaving badly as a criminal act. To avoid that, safe harbors can be added to legislation to limit liability in certain cases and situations.

Market bias is corrected. Stricter privacy laws don't stifle innovation or prevent online companies from sending targeted offers to consumers. Rather, they shift control from industry to individuals by requiring businesses to demonstrate that consumers approve of the way their information is being used.

Good business practice is incentivized. In a world where information has great value, it is common sense and good business practice for organizations to know what personal information they hold, to have internal controls on how it is processed and to make sure information is being used fairly. Strict, comprehensive privacy standards like those found in Europe motivate companies to adopt such practices and review them regularly to avoid punishment for misbehavior.

Redress is available. In Europe, individuals can take action when their privacy is violated. In the U.S., remedies exist only in targeted areas. For example, if a doctor discloses a patient's medical condition, the patient can sue under the health-information privacy law, but if a website discloses the same information, the web user has no claim. The lack of consistency undermines public trust in online activity and

JOHN WEBER

leaves victims legally helpless.

Independent oversight is provided. Oversight is critical if privacy rules are to have real meaning. An independent board helps ensure that the implementation of privacy principles in the dynamic and complex online environment is fair to both citizens and industry.

The flow of information is guaranteed. The European rules limit data exports to countries with insufficient privacy protection, which creates a serious problem for data transfers to the U.S. And as other regions adopt Europe's approach, complying with foreign laws is becoming more difficult for U.S. businesses.

Some say Washington can't be trusted with crafting complex privacy legislation and that the market, if left alone, can correct many of the flaws inherent in our current system. I disagree. Washington may be stymied by gridlock, but privacy tends to have bipartisan support and polls show that most Americans want more legal protections.

The U.S.'s experiment with self-regulation has failed Americans. We need a robust, legally enforceable Privacy Bill of Rights in the U.S.

Dr. Reidenberg is the Waxberg Professor of Law and the founding academic director of the Center on Law and Information Policy at Fordham Law School in New York. He can be reached at reports@wsj.com.

No: Stronger Privacy Rules Could Squelch Innovation

By Thomas H. Davenport

A push by the European Union to make its already-tough privacy laws even tougher, and to extend them to any company that collects data on EU citizens, has sparked renewed debate about whether the U.S. needs stronger data-privacy laws, too.

The U.S. now has fairly restrictive rules governing the collection and distribution of health and financial data, but few constraints in areas such as online marketing. Some people believe the U.S. needs to emulate Europe's approach and regulate the collection

Thomas H. Davenport *RUSS CAMPBELL*

and trafficking of all types of personal data.

I think that's a bad idea. Although I'm not a committed believer in the eternal wisdom of markets, in this case the market-based approach has advantages.

To be sure, sensitive health-care and financial information must continue to be heavily restricted. I'd even argue for greater penalties for data breaches than we have today. Privacy laws and penalties for breaches for children's data also should remain strong. But before we rush to restrict the use of all kinds of personal information, we have to consider that there is both a downside to stronger and more consistent privacy legislation and an upside to leaving it relatively weak.

We Can't Trust Them

The downside to stronger laws is that the current Washington incumbents—particularly those in Congress—can't be trusted to do a good job of crafting privacy legislation. If they can't pass a budget or a debt-ceiling increase, they have no business venturing into complex online privacy issues. It is unlikely that Congress could achieve consensus, but if it did, I suspect the outcome would be a bad law. The White House last year proposed a Consumer Privacy Bill of Rights, but it's only a voluntary code of conduct. Its very existence implicitly acknowledges that effective legislation from Congress is unlikely.

Tale of the Tape | Data Privacy in the U.S.

FUNDAMENTAL RIGHTS The word "privacy" doesn't appear in the U.S. Constitution, so ideas about the concept of privacy have developed over time in the courts. In general, the courts have focused on the idea of privacy as protection from the government, as in the Fourth Amendment prohibition on unreasonable search and seizure, or the First Amendment right to free speech and assembly.

THE LAWS The U.S. doesn't have a universal privacy law. Instead, it has a few laws protecting sensitive data, such as medical records and financial information. There are also separate privacy laws for things such as children's online data and even video rental records.

INTERNET RULES The U.S. has no laws requiring permission for online tracking. Instead, the country relies on a system known as "notice and choice," which means that companies disclose their practices in a privacy policy, and users can read through the various policies and decide whether to use sites based on that information.

STATE BY STATE States in the U.S. have different privacy laws. California, for example, has the Online Privacy Protection Act, which requires sites that collect personal information to have a privacy policy. Sites also have to tell users how they can review and make changes to their information. The state's attorney general recently said the act also applies to mobile apps.

REGULATORY POWERS U.S. regulators can take action if companies violate one of the separate laws on sensitive data. When it comes to general privacy, regulators can act if a company has done something in violation of its own privacy policy. But if the company discloses its actions in the privacy policy, the government is rarely able to fine it. Consumers also can sue companies over privacy violations, but they have had a difficult time winning money in court, mainly because it is difficult for people to demonstrate that they have been harmed monetarily. In general, the U.S. relies on the Internet industry to regulate itself by agreeing to certain standards.

—*Jennifer Valentino-DeVries*

The upside of lax privacy regulation, meanwhile, is innovation. The promise of using online data for marketing has always been that consumers would receive targeted benefits of value to them. Granted, it's pretty rare to receive offers we really value, but it happens.

Caesars Entertainment Inc., for example, has very extensive information on its customers' gambling habits and vacation preferences—

more than most loyalty programs, and certainly more than most online sites. Yet Gary Loveman, the company's chief executive officer, says customers never complain about how the information is used. Why? Because Caesars provides value in its offers—free dinners and shows if you're a frequent, valuable customer, and incentives to get to the next level of play if you aren't. Many of us would be happy to trade a little privacy in return for offers that really meet our needs, but companies like Caesars might have to abandon them altogether under more stringent legislation.

And let's face it, Americans don't seem too worried about the negative consequences of lax online privacy. Yes, it's easy to find out a lot about almost anyone online, but many of us make it easier with Facebook profiles, tweets and blog posts.

Transparency Is Key

For a market-based approach to privacy to work, however, companies must be transparent and consistent. They have to inform their customers what they plan to do with their data, and whether they will pass it along to other organizations—and no, they can't change the policy after collecting personal information.

It would be a good thing if there were legislation to make such transparency required and to penalize online companies that don't honor "Do Not Track" buttons on Web browsers, but I doubt we will get it from this Congress. Therefore, consumers will have to motivate businesses to adopt good business practices by gravitating toward companies and websites that explain their information-gathering practices in clear English and abandoning those that don't.

Those who think we need stricter privacy regulation in the U.S. say emulating Europe's approach would help online companies by ensuring the free flow of information internationally. While I agree that there is some benefit in privacy regulation that is consistent across time and place, that won't be what determines the success of online companies in the U.S.

Indeed, as this area continues to evolve, the most successful businesses will be those that are the most nimble and most able to treat different customers differently. Whether they reside in Birmingham, Ala., or Birmingham, England, will be just another difference.

Mr. Davenport is a visiting professor at Harvard Business School. He can be reached at reports@wsj.com.