Should you be sitting in cash right now?

If you have a \$500,000 portfolio, download the latest report by *Forbes* columnist Ken Fisher's firm. It tells you where we think the market is headed and why. This must-read report includes research and analysis you won't find anyplace else.

Don't miss it!

Click Here to Download Your Report!

FISHER INVESTMENTS

Dow Jones Reprints: This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers, use the Order Reprints tool at the bottom of any article or visit www.djreprints.com

See a sample reprint in PDF format.

Order a reprint of this article now

THE WALL STREET JOURNAL.

WSJ.com

JOURNAL REPORTS

Updated March 8, 2013, 1:36 p.m. ET

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

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.

Journal Report

Insights from The Experts

Read more at WSJ.com/LeadershipReport

More in Unleashing Innovation: Big Data

How Big Data Is Changing the Whole Equation for Business

Big Data, Big Blunders

The New Shape of Big Data

Moneyball, VC Style

A Guide to Facebook's Privacy Options

Vote

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

Thirty-five years ago, a federal commission studied



David Wentworth/Fordham Law School

Joel R. Reidenberg

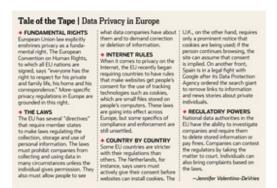
privacy protections in the U.S. and concluded that "neither law nor technology now gives an individual the tools to protect his legitimate interests in the records organizations keep about him."

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 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



John Weber

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 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 <u>reports@wsj.com</u>.

No: Stronger Privacy Rules Could Squelch Innovation

By Thomas H. Davenport



Russ Campbell

Thomas H. Davenport

A push by the European Union to make its alreadytough 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.

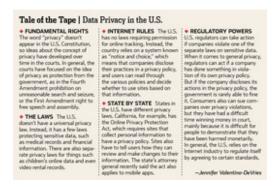
The U.S. now has fairly restrictive rules governing the collection and distribution of health and financial data, but few constraints in areas such as online marketing. Some people believe the U.S. needs to emulate Europe's approach and regulate the collection and trafficking of all types of personal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



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 <u>Facebook</u> 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 <u>reports@wsj.com</u>.

A version of this article appeared March 11, 2013, on page R7 in the U.S. edition of The Wall Street Journal, with the headline: Should the U.S. Adopt European-Style Data-Privacy Protections?.

Copyright 2012 Dow Jones & Company, Inc. All Rights Reserved

This copy is for your personal, non-commercial use only. Distribution and use of this material are governed by our Subscriber Agreement and by copyright law. For non-personal use or to order multiple copies, please contact Dow Jones Reprints at 1-800-843-0008 or visit www.djreprints.com