# US companies may need to beef up data privacy – but only for Europeans

12 April 2016, by Wade M. Chumney, California State University, Northridge

Can the EU and the U.S. work together on data privacy? Credit: shutterstock.com

Though the recent Apple versus FBI case garnered greater media attention, a privacy discussion with more economic significance – to the tune of US$260 billion – is moving toward fruition with less public attention: the EU-U.S. Privacy Shield.

To protect individuals' personal information, governments enact rules about how private companies must safeguard their customers' personal information. Because the rules differ between the European Union and the United States, U.S. companies that collect, transfer and store EU personal data must find ways to obey the appropriate rules.

This gets particularly thorny when dealing with personal data about customers. As a result, the respective governments have negotiated an agreement for how companies should act, so everyone is sure the rules are being followed.

Fifteen years ago, the EU and the U.S. finalized such an agreement, called the Safe Harbor, enumerating a list of principles with accompanying guidelines that companies had to promise to follow in order to be allowed to transfer data between the continents. But in October 2015, the top court in the European Union ruled that the Safe Harbor was invalid, saying U.S. privacy laws are more lax than European standards and U.S. mass-surveillance programs violate fundamental human rights established in the EU.

In its place, the Privacy Shield has been proposed, largely requiring the higher privacy protections provided by European law. Already approved in the U.S., it awaits ratification from the European Union. Recent document leaks suggest it may meet more resistance than previously expected. (In the meantime, temporary agreements keep data flowing across the Atlantic.)

If ratified, the EU-U.S. Privacy Shield will apply only to data privacy for EU citizens. However, if U.S. companies choose to make those standards applicable to all customers, U.S. citizens could reap the same benefits. It also reflects the need for international cooperation on data privacy in our technologically intertwined world.

**Differing views on privacy**

The differences between privacy approaches in the EU and U.S. are a reflection of history.

As a result of repressive regimes over the centuries, the EU has determined that privacy and security over personal data protection are fundamental rights.

The U.S., by contrast, has opted to allow market forces to shape privacy policy, so it lacks an overarching federal privacy law, opting instead for approaching the problem industry by industry, which generally leads to less privacy protection for U.S. citizens.

Bridging the gap between those two standards is the Privacy Shield, the full text of which was released at the end of February. It sets more

stringent rules than the now-defunct Safe Harbor, and indeed demands more than American law requires.

**What's different**

Generally, the new approach requires more of U.S. companies that collect, store and transfer Europeans' personal data. They must agree to several privacy principles, and take specific steps to follow them.

Some examples include:

- A mechanism by which consumers can complain about how a company has handled personal data. Companies must have an internal team to handle consumer complaints, publicize the team's contact information, resolve disputes without charging for complaints and respond quickly. In addition, companies must publicize the existence of a new independent process for reviewing complaints that consumers can't get resolved by the company directly.
- Heightened protection for data transferred from one company to another, requiring that the same privacy protections apply, and potentially holding the company that collected the data in the first place responsible for any problems.
- Retain records about the implementation of the privacy practices related to the Privacy Shield and make them available upon request.

More broadly, a significant change in the approach to privacy protection is a move from self-regulation under the Safe Harbor to an oversight system under the Privacy Shield. Federal agencies, including the Department of Commerce and Federal Trade Commission, will monitor and enforce compliance of U.S. companies. Additionally, the Department of State will establish an ombudsman to address concerns about U.S. government surveillance and gathering of European citizens' personal data.

EU and U.S. officials hope that changes such as these will meet the European privacy standards required by the top court in the European Union after the Safe Harbor was invalidated.

**Taking effect**

The U.S. has already done its part to put the agreement into effect. What remains before it's finalized is on the European side.

European authorities have already announced that the Privacy Shield would adequately protect the personal data of EU citizens. But the administrative process needs to play out first, with completion expected by the summer.

In anticipation of the Privacy Shield potentially taking effect later this summer, U.S. companies committed to doing business in Europe would be wise to adopt its more stringent privacy rules. Doing so would not only prepare them to meet the new standards, but would also limit their vulnerabilities to data-privacy breaches within the U.S. Improving data privacy for U.S. customers might even garner goodwill on this side of the Atlantic.

*This article was originally published on* The Conversation*. Read the* original article*.*

Source: The Conversation