

Coping with Europe's data blockade

Jay Cline

December 17, 2002 ([Computerworld](#))

Getting ready to pull customer data out of Europe? Be prepared to navigate the most backward regulation in the data privacy arena.

The European Union has declared that countries without privacy laws like its own -- the U.S. included -- are "inadequate" places to store a European citizen's personal data. Brussels threatens to fine your company if you try to export such data past its blockade without meeting its conditions. This isn't about privacy. The safety of a person's data has little to do with where it's stored. Is a database server in Lisbon necessarily safer than one in Silicon Valley? Geographic location is almost meaningless in cyberspace. What matters in the information economy is whether the company collecting the data can be held accountable in a court for violating a posted privacy policy.

The EU's move isn't about privacy, but about the power of government to regulate the trade of the 21st century's raw material: information. By forcing other countries to adopt its laws, the EU hopes to isolate the U.S., home of the great IT innovators. It's no accident that Brussels targeted the goliath Microsoft for a privacy investigation of its Passport product.

So what do you need to do to spring your data from Europe?

Your short-term options are several, but unattractive. You can avoid the EU export requirements altogether by keeping the personal data you collect in Europe within European Economic Area borders. Maintaining a duplicate IT infrastructure in Europe may not be feasible for you, however.

A second option is to "depersonalize" the data before exporting it to the U.S. This involves stripping personal identifiers from the data so that no one in your U.S. office could trace the information to named Europeans. Arguably, personal data that is merely stored in the U.S. but not accessed here should fit this category as well. This option works only if your U.S. office has a narrow role, such as analytics or data backup.

A third alternative is to obtain the consent of your European customers to export their data to the U.S. While easy to engineer -- by adding a pop-up box to a checkout process, for example -- the hard part is planning for those people who won't give their consent. You'll either have to accept them abandoning the checkout process or create a duplicate fulfillment process based in Europe.

Another option is available if you have a European office or business partner that can collect the data for you. In order to export the data, both parties would have to sign a "transborder data flow agreement" verifying that the data will be processed according to the EU's data protection principles.

In the short term, then, navigating through the EU data blockade will be costly or even infeasible. The European Union has effectively created a nontariff trade barrier that has little to do with personal privacy, but much to do with trade regulation.

If data collection in Europe is a key part of your business strategy, your long-term plan should include joining the ["safe harbor"](#) program. To do so, complete a U.S. Department of Commerce form declaring that your data practices conform to the seven safe harbor privacy principles, and verify that they do. You'll probably need to create an independent-recourse process for consumer complaints.

If the Commerce Department accepts your application, all of your systems can export personal data from Europe to the U.S. without the need for special contracts or customer consents.

The safe harbor program covers only U.S. companies, however. What about Japanese or Australian firms? There is no silver bullet yet. Trade officials in these countries should consider joining with the U.S. and EU to create a worldwide safe harbor. The emergence of a global safe harbor network would be a face-saving way for all parties to claim victory and tear down the walls that restrict the free flow of information.

Europe once joined with the U.S. to champion the liberalization of world trade. The challenge is upon them to reaffirm those hard-fought ideals.

Cline manages data privacy at [Carlson Companies Inc.](#), a Minneapolis-based group of businesses in the travel, hospitality and marketing industries. Contact him at privacy@computerworld.com.