ACAMS | MONEY LAUNDERING.COM

In Growing AML and Privacy Demands, Banks Find a Quandary, Says Author

December 12, 2014

As the European Union weighs a new raft of data protection standards, some bankers believe that they can't meet both anti-money laundering demands and Europe's privacy expectations, according to Michelle Frasher, author of the forthcoming *Information Statecraft: States, Financial Institutions, Individuals and the Politics of Counter-Terrorism Data*.

Under a proposed bloc-wide directive, EU member-states would adopt uniform standards to limit the sharing of personal data, including financial information. But since a $1.9 billion settlement with HSBC USA in 2012 for failing to monitor trillions of dollars in wires, banks with American operations have conversely faced pressure to share compliance information with their operations abroad.

That tension could soon worsen. The EU's Data Protection Directive would place new demands on U.S. multinational banks, possibly requiring them to overhaul their compliance programs, according to Frasher, who is studying the topic for the Society for Worldwide Interbank Financial Telecommunication, or Swift.

Frasher recently discussed these issues with *ACAMS moneylaundering.com* senior reporter Colby Adams. What follows is an edited transcript of their conversation.

Describe the book you're writing and how financial intelligence has become more important to governments. How has its value changed historically?

I started looking at money as data—just as data on its own, not as a reflection of wealth, which is how we typically look at it, wealth and value. All data theoretically has some sort of intelligence value, but money is pretty unique. You look at the financial services community, you see how global it is and you realize that that data has the ability to reflect behaviors beyond investment.

The book argues that the control of financial data—all data really—is a form of information statecraft, a tool that nations are increasingly using to leverage their power internationally. Obviously, to get that data you need financial institutions to give it to you through compliance or subpoena, or you have to tap into the information networks that hold it in other jurisdictions. We've seen both.

The financial services community looks at behavioral trends all the time when

they're assessing clients, matching their needs to services in hopes of securing new lines of business. Governments do the same thing, matching funds transfers and other financial behavior to intentions. In fact, they profile in much the same way and obtain the same data, but for different reasons. The third group involved is individuals who produce this data, consumers like us.

So the book is really about looking at data in this technological age that recognizes very few boundaries, and the conflicts in the transfer of data between those three stakeholders and how they deal with conflicts in privacy and national security laws across the U.S. and Europe.

When did you first become familiar with Swift?

Swift was involved in perhaps the most high-profile, very public instance of financial data's collection for intelligence purposes within the Terror Finance Tracking Program, [first disclosed in December 2006]. The conflict between its collection and the EU's data privacy and protection standards hasn't disappeared. Rather, it has also placed new emphasis on long-term problems, such as how financial institutions can comply with the EU's and U.S.'s very different regulatory regimes.

Last year, I spent four months in Europe as a Fulbright-Schuman Scholar, a program sponsored by the U.S. State Department and European Commission that supports research of interest to the transatlantic policy community. I spoke with private bankers, compliance officers, central bankers and IT sector professionals, and noticed that there wasn't a clear understanding of how the politics was affecting their operations. And there wasn't an understanding on the political and regulatory side about how banks managed their data and the lengths to which financial institutions were going to obtain and transfer customer data while complying with U.S. and EU privacy or national security laws.

For Swift, I'm producing an overview of the conflicts between [anti-money laundering, or AML] reporting and privacy laws that govern cross-border data flows. The bankers and compliance officers I've interviewed thus far do not believe it is possible to meet regulatory data protection and privacy expectations while transferring all of the data they'd like to transfer, for risk management purposes, between their branches and affiliates in different jurisdictions. This conflict has left them very exposed to enforcement and prosecution, and has cut deeply into their budgets.

So I'm looking at how banks construct their compliance teams to deal with this conflict and looking for avenues of cooperation to help efficiency. For example, have they integrated certified privacy professionals inside their AML function, are those persons also certified for AML purposes and where are the IT security people?

We've reported on some of the workarounds that financial institutions have crafted to circumvent the problem. What are the advantages and

limitations of "binding corporate rules," which allow banks to more freely share data under policies approved by governments?

If you're a finance multinational, you have a few choices to manage data transfers. Binding corporate rules (BCRs) require an internal plan, assessing what your data is and how you plan to use it. Then you have to put this plan together about how you're going to share it among your affiliates and subsidiaries. Then you have to obtain approval from the data protection authority in every EU country in which you have business, though there are some EU countries that will automatically accept a BCR once another has approved it.

The silver lining for U.S. firms is that, while they are crafting a BCR, they are taking inventory of their data collection, transfer and management processes, including domestically, so that they can comply with the patchwork of data rules in the United States. The arrangements don't invalidate other cross-border transfer certifications like Safe Harbor. Corporations can customize BCRs to the type of data they want to include and limit their jurisdiction, too.

BCRs are controversial because they aren't mandatory under the directive and corporations fear that that their investment [in BCRs] won't be honored in the pending regulation, but there is strong support for a grandfather clause, which is the likely result. Also, the directive and BCRs put the risk, responsibility and accountability on the "controller"—for our purposes, the financial institution—that outlines how sensitive information such as [know-your-customer, or KYC] data would be collected, used and processed.

The "controller" usually hires "processors," [defined as the entities that process personal data on behalf of the controllers], but the processors aren't held as accountable for what happens to the data. So for banks and other firms to outsource this important task, which is commonly done and becoming more and more so, is risky.

In 2003, [an independent EU advisory group] outlined BCRs for controllers. Then people said, 'well it's not fair to put all of the onus on controllers, so let's even it up. Let's put some rules in place for processors.' The 2012 proposal for the regulation tried to bring more accountability to processors with their own BCR process, but it was removed from the regulation by the EU Parliament, which feared it would be used as an excuse, as a loophole for whichever part of the firm is receiving the data overseas to hand it over to their domestic government, and then the parent company, the original crafter of the BCR, would be off the hook. This [reluctance to allow companies to share such data with their home governments] is one example of how Edward Snowden affected the pending regulation.

What is the worst-case scenario in terms of the pending EU data protection regulation?

We're already in a worst-case scenario, with zero uniformity in various national data protection regimes. Some people are arguing that the new regulation may even streamline the process for banks and make data transfers a lot easier overall, even if the data protection laws in individual EU countries are more stringent than what is required by the eventual EU regulation.

But wouldn't that be the same problem that financial institutions must deal with under the current directive? EU countries like Germany have much tougher rules than other EU members, so again you have a patchwork of rules to comply with.

The issue that U.S. banks need to look out for is whether the final regulation will allow for a 'one-stop shop,' meaning one EU-wide data protection authority having final say over whether a transfer of data is valid. The EU Council has most recently proposed that national data protection authorities must retain some power, but how much power they will have to veto certain information-sharing plans—for example a bank's plan to transfer KYC data overseas for risk management purposes—is still up for grabs. The Council is still discussing the text voted on by the Parliament. They are debating whether to allow national data protection authorities some sort of say, so they are making allowances for national concerns.

The other question is how would they detect a breach of the expected regulation?

That depends on what kind of breach. When we are talking about data protection, we are talking about commerce-related data. That regulation, very minimally, addresses data that the government uses for national security or that the police uses for criminal or terrorism investigations. This is where AML professionals are walking a tightrope because, on one hand, they are dealing with commercial data but, on the other, that commercial data may indicate illicit finance and its reporting is covered under different, but overlapping regulations and laws.

Counterterrorism finance invoking national security concerns and tracking the funds can be used to identify who is using them to fund violence, as well as who is financially supporting that activity. So when you cross over from that data being used in a financial or commercial way, as the directive and the regulation are aiming for, to a police or national security investigation, the laws and standards may change. I stress 'may.' It's still unclear.

So we're talking about apples and oranges at this point.

Yes, but they're smashed together, and that's where the tightrope is. AML professionals collect this data to varying degrees of thoroughness, for run-of-the-mill checking accounts to private bank accounts held for politically exposed persons. But those data protection rules [promulgated since 1995 under the Directive] still apply, in some cases, to AML reporting across borders. This is why disqualifying processors

from information-sharing arrangements like binding corporate rules is significant. The EU is signaling that they are concerned that commercial data, once transferred abroad, could end up in the hands of national governments and used for national security purposes.

Right now, the European Union is also talking about whether they want to put together a directive for the collection of police and national security data. This is all with the intention of melding these two issues together under one legal roof, eventually.

How does blurring the line between how commercial- and security-related data is shared impact bank compliance officers?

It places your readership in a very difficult position because they have to realize that different rules may apply when you're reporting something for KYC purposes, for AML purposes and for counterterrorism financing purposes.

All these data protection discussions are going on while the EU is also debating the overhaul of the Fourth Anti-Money Laundering Directive, and hopefully making sure those two objectives [the Data Protection Regulation and the Fourth AML Directive] don't conflict before they are finalized.

Neither is likely to completely solve—and hopefully neither will worsen—the dilemma created by suspicious activity reporting and the expectation, at least in the United States, that such information should be shared without exception. The problem is the nature of the [suspicious transaction report, or STR]. You're not necessarily reporting a crime or terror finance. You're reporting a suspicion, so that may not trigger any kind of national security exception. Or suppose you are filing a suspicious transaction report on suspected tax evasion versus an STR for money laundering or terrorism. It's not clear what rules will apply, which also means your risk exposures will change.