Bridging the Gap: Europe vs America AML / CTF and Data Privacy Law

Michelle Frasher

2014 Fulbright-Schuman Scholar & Research Fellow

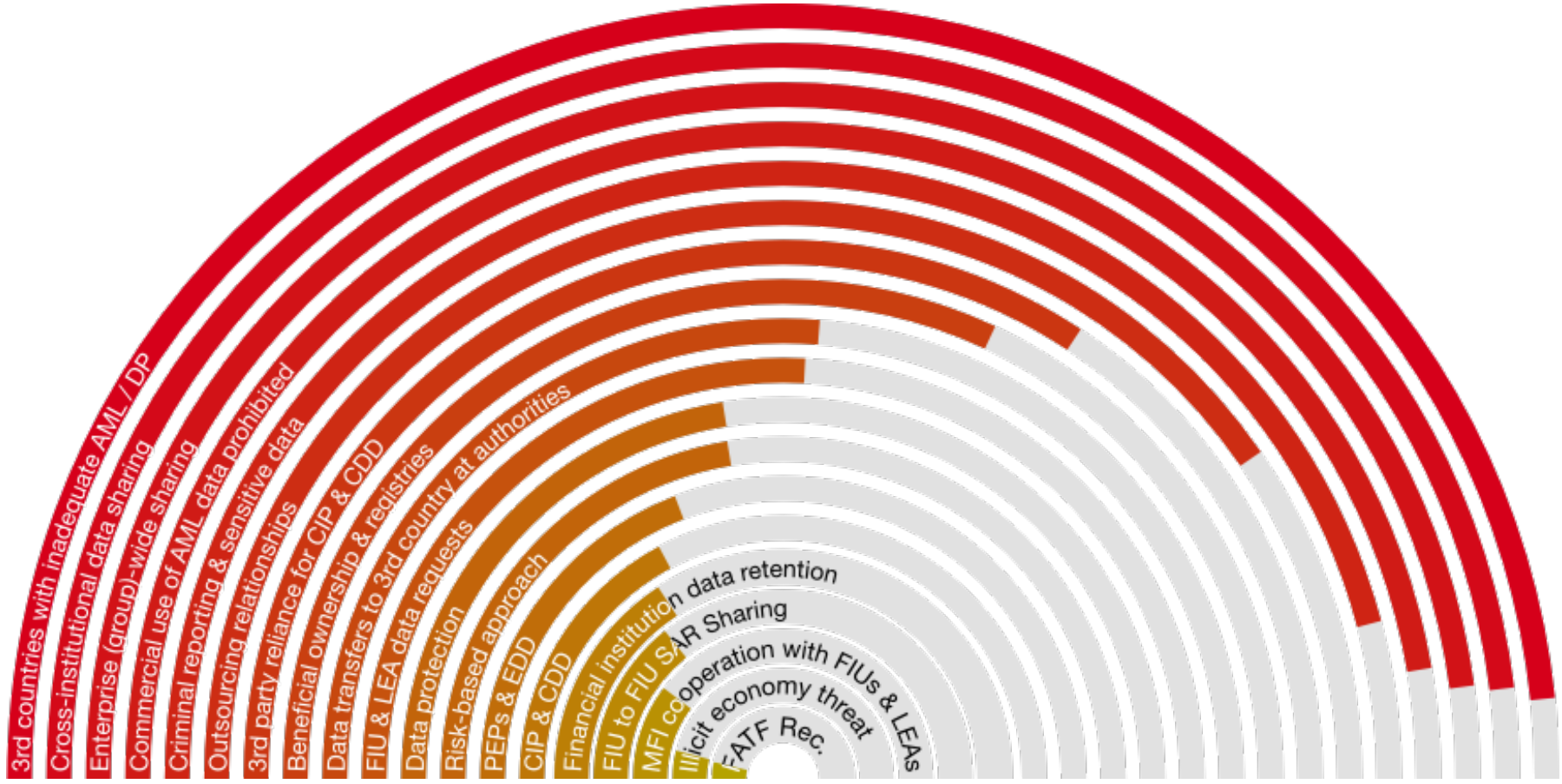
Information Statecraft

- Where states attempt to influence, through law and technology, the acquisition, control, or presentation of data, information or knowledge to extend their political, social, security, and cultural policies across issues and borders.
- ***States*** use financial data to map behaviors and expose the illicit economy and networks of political violence.
- ***Financial Institutions*** use data to create businesses strategies, empower trading capacity, determine client and market behaviors and to produce profits.

The Duality of Financial Data

“…the collection of data for anti-money laundering purposes takes place at the same time as the collection of data for commercial purposes.”

19 Challenges between US and EU AML/CTF Compliance and Privacy Laws

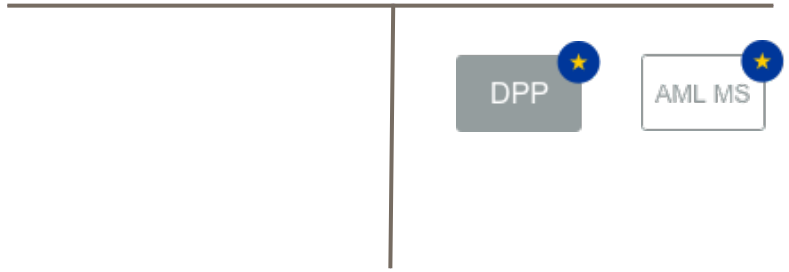


Prohibition of AML Data for Commercial Use

HIGH SEVERITY

Europe's group-wide AML and data protection requirements impact all EU and US firms in some capacity. EU and US banks may engage with high-risk markets, but EU firms must put in place EU AML and data protection policies to satisfy EU regulators; US companies must establish US level AML programs while complying with local regulations. The GDPR holds firms accountable for any data transferred to a third country, including onward transfers.

Privacy Conflicts

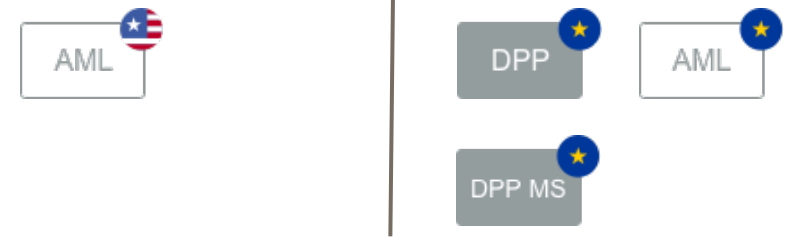


Enterprise (Group)-wide Sharing – SARs & Supporting Data

HIGH SEVERITY

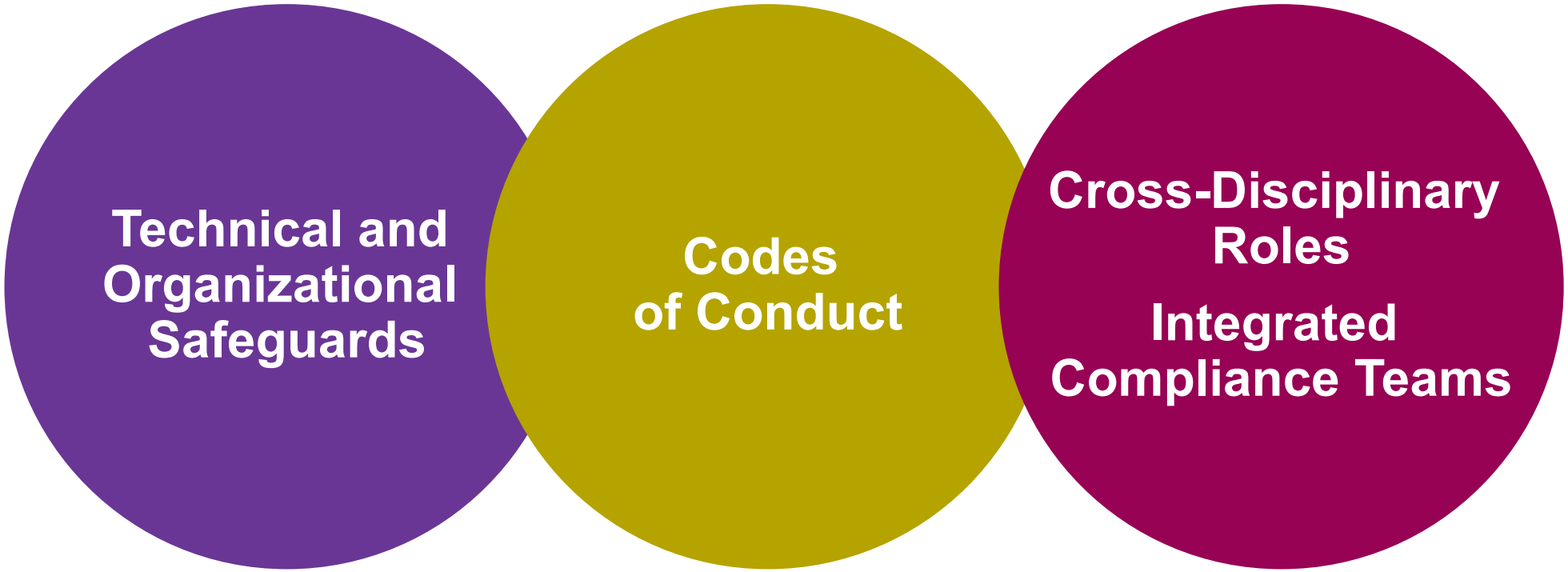
The conflicts between US and EU views on enterprise-wide SAR and underlying data-sharing present one of the greatest obstacles to a cohesive AML compliance strategy. When foreign branches, subsidiaries and affiliates cannot access and share enterprise data they cannot see client, transactional, or behavioral links across their businesses, which can create repetitive or incomplete reports to national authorities. The report found that both US and EU laws impose legal controls that inhibit data flows.

Privacy Conflicts



Profiling and Automated Processing

Next steps


Technical and Organizational Safeguards
Codes of Conduct
Cross-Disciplinary Roles
Integrated Compliance Teams

Questions