



Data Privacy Meets a World of Risk

A Landscape in Turmoil

The Fluid Privacy Landscape

- Shrems v. Data Privacy Commissioner – October 2015
 - Safe Harbor ruled unenforceable
 - Years worth of policy, practice, asset configuration thrown out in a moment
 - Immediate, powerful uncertainty as to immediate consequences, long term effects and strategies
- General Data Protection Regulation – Q1 2016
 - Announces “Data Shield”, the replacement for Safe Harbor
 - Introduces a “harmonized” privacy regulation regime to give organizations some uniformity and certainty throughout the EU



Safe Harbor Gives Way to Privacy Shield

- In theory, a better, easier way to manage data transfers between the EU and US
 - Similar or better levels of protection
 - More accountability
 - Mechanisms for recourse and redress in cases of violation
 - Less access by the US government
- In practice, not so much
 - Self-certification mechanisms much the same
 - Shrems has already indicated he'll litigate



Key Points of the GDPR

- Intended to provide a uniform privacy regulation framework throughout the EU
- Many prior responsibilities and requirements remain in place and in effect
- Establishes for each organization, a “home” DPA to work with
- Reaffirms the absolute independence and plenary authority of the DPA's
- Encourages, but does not require, national DPA's to coordinate and cooperate on harmonizing requirements
- Leaves all current regulation in place unless and until national DPA's elect to revise/replace/repeal



Where Did We Stand?

Then

- DPA's had plenary authority
- Rulemaking on a country-specific basis
- No cooperation or coordination between DPA's
- Widely varying rules and practices
- Some certainty via Safe Harbor
- Uncertainty due to litigation threats



Where Do We Stand?

Now

- DPA's have plenary authority
- Rulemaking on a country-specific basis
- No required cooperation or coordination between DPA's
- Widely varying rules and practices
- Some certainty via Data Shield
- Uncertainty due to the threat of litigation

GDPR and Data Shield Bring Little Relief

So what's Changed? Not much, really

- DPA's may elect to cooperate. Maybe not.
- DPA's may harmonize rules and enforcement. Maybe not.
- DPA's may remove some of the sillier/unrealistic requirements. Maybe not.
- All this will take years to shake out

And all of that is in the future. Right now, it is for all practical purposes the same landscape we had before.

- Except that it could change at any time.
 - DPA's writing rules
 - DPA's ramping up enforcement
 - Schrems et al litigating

But What Else Has Changed?

The world.....

Europe, far more than the US, has been subjected to terrorist attacks

- Shootings
- Bombings
- Vehicle assaults
- Bladed weapon attacks

Europe has had a tough time responding and containing this trend, in part because of stringent data privacy laws

- Tough to gather information
- Tough to keep information
- Tough to share information
- These laws apply to law enforcement



The Fundamental Tension between Personal Rights/Privacy and Security

- The concepts are inherently opposed to each other
- The less the government knows or can find out about you, the more secure you are in your personal liberty and privacy
 - The problem is, this applies to criminals/bad actors/terrorists as well
- The less the government knows about criminals/bad actors/terrorists, the less able it is to avoid/ thwart/punish their conduct
- In order to know more about criminals/bad actors/terrorists, the government must necessarily know more about people in general
- The only question is how to strike the correct balance



The Cost of the Balance

- Simply put, lives
 - More personal liberty/privacy costs some number of lives lost that would otherwise not be lost
 - Every additional increment of liberty/privacy we choose to grant ourselves adds to that cost
- The flip side
 - Adding security exposes us:
 - Investigation
 - Embarrassment
 - Harassment
 - Repression
 - Any increment of personal freedom/privacy involves deciding how many lives are worth it



The EU Conundrum

Have we gone too far in protecting personal privacy?

- It's easy to take an extreme position when the lives in question are theoretical, or you simply ignore them
- The question is harder when the lives lost are many, and are lost in your city, your train station, your airport
- It's harder still when only good fortune cause the incident to happen when you or your family were not there



What Can the EU Do?



- Major players – France, Germany – are actively re-thinking the privacy question
 - many it's time to pull back
- Many countries are experiencing an electoral backlash
 - Conservative, nationalist, pro-security candidates are running well
- Legislation, rules
 - Can be revised, but:
 - Changing the legislative framework very, very slow
 - In the absence of significant changes to the legislative framework, DPA's won't change existing regulation

The Question of Enforcement

In the short term

- Laws are what the courts and regulators say they are
 - Enforcement is the tip of the spear, and it happens when and where the DPA's and courts say it does
- They can choose to enforce privacy laws aggressively, selectively or not at all, and they are answerable to no one
 - And they, and their families, are just as much at risk as anyone else
- So, the short-term solution may be to simply choose a different enforcement course for existing privacy law



The Question on Non-Enforcement

Not so different, really

- Enforcement has always been something of a charade
- Impossible rules
- Poor understanding of them
- Uninformed self-certifications
- Enforcing only in egregious/high profile cases



The Effects on Future Litigation

- Schrems will sue, but . . .
 - Courts may take a different attitude
 - Legislators may beat him to the punch and change the rules
 - Regulators may simply decline to enforce, regardless of any court ruling



Where does that Leave Us?

- Lots of uncertainty, but:
 - Data Shield is there, take advantage of it
 - Do what you can to avoid potential future problems
 - Don't collect or keep data you don't need
 - No data transfers outside the EU that aren't really necessary
 - Configure new systems with data privacy in mind
 - Contact your home DPA. maybe they'll actually do something
 - Avoid committing to expensive solutions until the air clears
 - Expensive new systems and controls
 - Major reconfiguration of existing systems and controls
 - Watch and wait – eventually the path will start to become clear

