

Economic Impact of European Reform of Personal Data Protection

FSR Annual Policy Conference – 28th May 2015

Marc Lebourges, Regulatory Affairs ORANGE

Disclaimer: personal positions, may not represent Orange positions



This presentation is to a large extent based on an article of my colleague Stéphane Ciriani:

“The Economic Impact of the European Reform of Data Protection”

published in Communications & Strategies review

Q1 2015

Outline

- **US dominance** in the EU OTT market and EU US different philosophy of personal data protection
- **EU privacy reform** aims at reinforce, harmonise & extend EU personal data protection, but it is accused of being protectionist.
- Will **EU privacy reform** impose asymmetric regulatory cost burden from the EU to the US? Not at all, but:
- **EU privacy reform** may not be economically efficient for the EU
- **Conclusion:** efficient regulatory balance between personal data protection & the development of digital services yet to be found by EU authorities and regulatory equity a powerful lever for it

US dominance of the OTT market in the EU

- US OTTs lead the ecosystem of services which monetise personal data (Intermediation, e-commerce, Big Data & Cloud, online advertising):

Google, Facebook & Amazon = 54% world Internet sector market value (without Apple)

Google has 86% market share of search engines in the EU.

16 US companies among 20 world largest Big Data vendors.

72% of cloud services provided in the EU store data in the US (as of 2014).

- EU Personal data value created in the EU essentially goes to the US OTTs.
- US OTTs do not have to install equipment in the EU to process EU data.
- EU personal data are widely transferred stored & processed to the US
- because of the US OTTs global domination

Different data protection philosophy EU vs. US

- Personal data protection in the EU: **Fundamental right**, not tradable, not subject to economic efficiency criteria.

Personal data protected under EU law:

Data protection Directive 95/46/EC under revision (GDPR)

E-Privacy Directive 2002/58/EC (Telecoms).

Processing of personal data is **a priori prohibited** unless proved to be useful

- Personal data protection in the US: **Property right** tradable on a market.
No general personal data protection law in the US.
Enforced on a **sector-by-sector basis** under the **FTC** authority.
Importance of self-regulation

Processing of personal data is **a priori lawful** unless proved to be harmful

- EU personal data transfers from the EU to “**non-equivalent**” countries: companies have to comply with the EU law:
(MCCs & BCRs), Safe Harbour (US considered “adequate” if SH is applied).
Safe Harbour based on companies’ notification to the **FTC**.

EU privacy reform's goals

- **GDPR:** creates a unique legal framework for the processing & the free movement of personal data in the EU (harmonisation of Member States' data protection rules).
- **GDPR** replaces **DPD 95/46/EC** with new protection rules: DPO, DPIA, Right to data portability, Right to be forgotten, sanctions up to 5% annual worldwide turnover, breach notification...)
- **Extraterritoriality Principle:** EU law applies to every service provider (whatever the nationality or the location) which collects, stores, & processes personal data of EU citizens.
- ➔ GDPR not only makes DPD harmonised and in theory enforceable outside EU, but adds regulatory substance

EU claims to defend principles & values but in reality tries to protect own economic interests against US leading competitors. Barack Obama, February 2015

- “In defense of Google and Facebook, sometimes the European response here is **more commercially driven than anything else.**”
- “But sometimes [EU] vendors — their service providers who, you know, can’t compete with ours — are essentially trying to **set up some roadblocks** for our companies to operate effectively there.”
- “We have owned the Internet. Our companies have created it, expanded it, perfected it in ways that [EU] can’t compete. And oftentimes what is portrayed as high-minded positions on issues sometimes is just designed to **carve out some of their commercial interests.**”

Impact assessments supported by the US: GDPR is a protectionist reform & hinders EU growth

- **US economic studies:**
 - EU's economy will benefit from a full liberalisation of EU-US data trade (optimal policy = personal data protection addressed within **TTIP** ; no revision of Safe Harbour & no adoption of GDPR).
 - US economic studies:
 - Are serious studies
 - However, analyse more the impact of an effective enforcement of existing DPD than the impact of new specific GDPR provisions (e.g. under GDPR, no need to install hardware in EU to be subject to EU law)
- **ECIPE (2013)** on behalf of US Chamber of Commerce :
 - 1) **GDPR adoption & more stringent Safe Harbour -1% in EU-US trade** in one year after adoption
 - 2) **GDPR adoption + Repeal of SH, MCCs & BCRs → -20% US exports to the EU & -1% EU-27 GDP.**
 - 3) + Application "Right to be forgotten" → **-4% EU-27 GDP.**
- **ECIPE (2014):** Adoption of **GDPR alone = -0.4% EU-27 GDP**
Adoption of **GDPR + Hardware localisation requirement → -1.1% EU-27 GDP & -3.9% EU-27 investment drop**
- **US industry lobbying:** opposed to EU "data protectionism":
GDPR adoption = Repeal of Safe Harbour, (MCCs & BCRs) = Requirement to install hardware in the EU to provide digital services to EU consumers.
- **US Trade Representative Office (2014):** Repeal of Safe Harbour = Requirement to install hardware in the EU = Blocking US OTTs leaders thought a shift of EU regulatory cost burden to the US industry.
- **HOFHEINZ & MANDEL - PPI (2014):** **GDPR = «Regulatory trade barrier»** to exclude US OTTs to foster EU digital champions (anticompetitive & protectionist purpose). Recommend to keep Safe Harbour as it is & reject GDPR.
- **EZELL *et al.* – ITIF (2013):** Requirement to install Hardware in the EU → Increase in production costs, decreases in profits & investments from US companies → Digital shortage in the EU.

GDPR is neither protectionist nor anticompetitive

- **Data Protection Directive 95/46/EC** was adopted before the creation & the rise of US OTTs with the policy scope of protecting EU citizens' personal information according to 1980 OECD Guidelines.

DPD was not designed to tackle EU commercial deficit in digital service trade.

- **The extraterritoriality principle** aims at harmonising rules for both EU and non-EU players; there is no transfer of regulatory cost burden to the US companies. **Both US & EU players** will apply the same protection rules when collecting, moving, storing, & processing EU personal data of EU individuals (Level Playing Field). **Does not suppose implementation of hardware in the EU**

But is the EU privacy reform economically efficient?

Commission view: GDPR increases global efficiency of data protection & fosters competitiveness of EU companies on foreign markets

- Harmonisation → **2.3€ billion efficiency gains** from reduced administrative legal burden (in one year after adoption).
- Extraterritoriality → EU-US level playing field in the EU: Same rules for every provider which processes EU personal data: EU & US compete on fair efficient ground in the EU.
- Competitive edge for EU providers on foreign markets:
better protection → higher consumer trust → Consumers' **more likely to adopt** EU providers' services → EU gain market shares

Does trust in data protection standards foster the adoption of digital services?

- **BCG (2014):** Economic value of data-intensive digital services = 8% of EU-28 GDP by 2020 (if consumers' trust in data protection standards high enough to foster adoption).
- **BRADSHAW *et al.* (2012):** Consumer trust in data protection standards fosters adoption of Cloud services (potentially 2.3% UK GDP by 2020).
- **ACQUISTI *et al.* (2006):** Personal data breaches hinder market value of publicly traded firms (NYSE & NASDAQ) over 2000-2006. (Day loss of 0.6%).
- **CAMPBELL *et al.* (2003):** Personal data breaches cause drop in stock market value of large US companies (NYSE AMEX & NASDAQ) over 1995-2000 (no negative market reaction in case of security breaches involving non confidential information).
- **EU Commission (2012):** GDPR fosters competitiveness of EU digital providers on foreign markets: more stringent, better data protection policies → increased levels of consumer trust → Increases EU providers' world market shares.

With the exception of EU Commission, impact assessments show inefficiency of GDPR

- **UK Ministry of Justice (2012):** GDPR gains from legal framework harmonisation < Regulatory burden from administrative costs → increases in UK corporate IT costs: net cost of **GDPR = £250 million after 1 year ; £2.1 billion after 14 years** (for the UK economy).
- **CHRISTENSEN *et al.* (2013):** GDPR adoption → Increases annual IT spending of EU companies (+20%) → Increases in unemployment (+0.3%) & Reduction in the number of companies in the UK economy (-3%).
- **PYKKO (2012):** GDPR imposes same protection rules for all sectors = Hurdles to the development of financial services → Tightened credit supply → Undermines investments & EU economic growth.
- **LLOYD CBI UK (2012):** GDPR increases regulatory cost burden within the EU & data protection rules' complexity ; Data portability undermines private incentives to invest in better services.
- **GOLDFARB & TUCKER (2011):** EU data protection law **DPD 95/46/EC** decreases efficiency of online advertising, & restricts ability to monetise digital services.
- **BUCHHOLTZ (2014):** Big data could increase EU-27 GDP by 1.9% by 2020 **provided that** EU data protection reform sets the right balance between protection rules & business opportunities to monetise personal data.

Consumer mistrust in data protection standards does not hamper digital services' adoption: GDPR might not be a competitive asset for EU companies

- **TADDICKEN (2013):** Empirical evidence of «Privacy paradox»: Consumer concerns on personal data protection does not hamper usage of digital services (social web).
- **US OTTs** are still world leaders after **NSA-PRISM** disclosures in July 2013 (Market dominance in internet services and Cloud infrastructure & services alike).
- **IDATE (2014):** Low levels of consumer trust in privacy protection standards does not restrict the intensity of digital services' usage (does not hampers adoption of services).
- Reinforced rules of personal data protection might not be enough for EU companies to gain market shares outside the EU.

GDPR is neither protectionist nor anticompetitive but might be economically inefficient for the EU

- EU has yet to find the right balance between **data protection rules** & flexibility required to **monetise personal data** & fosters innovation in EU digital services.
- GDPR should be improved:
 - rules for consent should be efficient
 - definition of personal data should be rigorous and not too extensive
 - Inefficient double responsibility of sub-contractors
 - disproportionate documentation obligations
 - disproportionate level of sanctions lead to legal uncertainty.
- Telecom e-privacy D should be repealed

Regulatory equity: a lever for balanced regulation

- Because of the absence of regulatory equity between EU and US provider,
 - EU policy makers may adopt disproportionate data protection rules, with no political cost;
 - as US providers are not really subject to EU laws, they continue to provide efficient services to EU users
- **Under regulatory equity**, EU policy makers would have to make balanced choices, as they will have direct effects on services actually available for EU users:
 - genuine search of balance between regulation and innovation, without outside option;
 - actual protection of end-users
 - fair competition between US and EU providers.

Thank you

