Data Transfer Without Safe Harbors

Ted Claypoole

Partner, Womble Carlyle

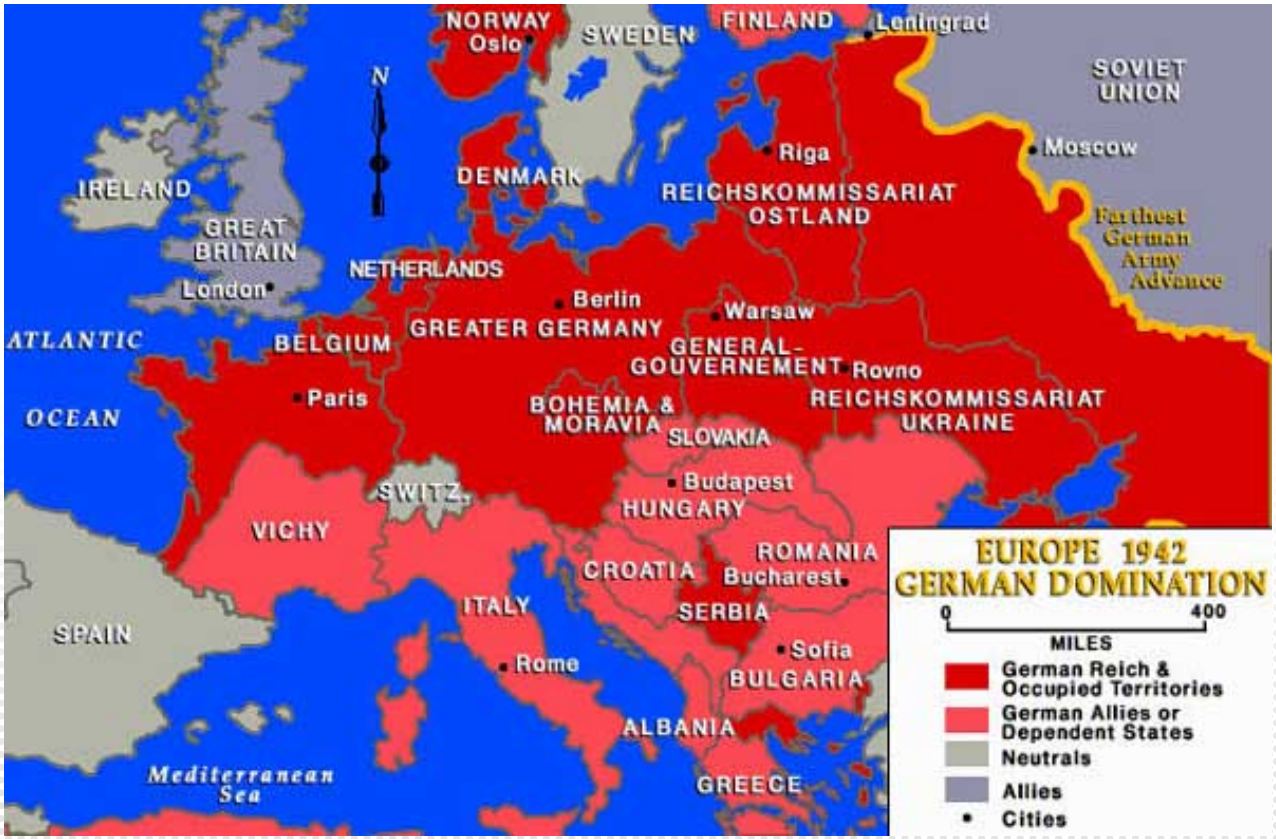
WOMBLE CARLYLE

What we will Discuss Today

- How did we get to this place?
- Where are we now?
- What comes next?

WOMBLE CARLYLE

Not so long ago



WOMBLE CARLYLE

Even Less Far Back

WOMBLE CARLYLE

European Union Positions on Data Use and Transfer

- All the member states of the EU are also signatories of the European Convention on Human Rights (ECHR). Article 8 of the ECHR provides a right to respect for one's "private and family life, his home and his correspondence", subject to certain restrictions.
- Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data)[EU Data Protection Directive]

WOMBLE CARLYLE

EU Privacy Directive 1995

- Safe Harbor provision
- Model Clauses for protecting Privacy
- Binding Corporate Rules

WOMBLE CARLYLE

EU Privacy Directive 1995

Article 13 Exceptions:

- Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6 (1), 10, 11 (1), 12 and 21 when such a restriction constitutes a necessary measures to safeguard:

  (a) national security;

  (b) defense;

  (c) public security;

  (d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;

  (e) a important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;

  (f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);

  (g) the protection of the data subject or of the rights and freedoms of others.

EU Data Protection Directive

OECD Seven Principles of Data Privacy (1980) – later incorporated into the EU Directive

- **Notice**—data subjects should be given notice when their data is being collected;
- **Purpose**—data should only be used for the purpose stated and not for any other purposes;
- **Consent**—data should not be disclosed without the data subject's consent;
- **Security**—collected data should be kept secure from any potential abuses;
- **Disclosure**—data subjects should be informed as to who is collecting their data;
- **Access**—data subjects should be allowed to access their data and make corrections to any inaccurate data; and
- **Accountability**—data subjects should have a method available to them to hold data collectors accountable for not following the above principles

Personal Data and its Use

- ***Personal data:*** "any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;" (art. 2 a)
- Personal data should not be processed at all, except when certain conditions are met. These conditions fall into three categories: **transparency**, **legitimate purpose**, and **proportionality**.

Personal Data and its Use

Personal data can only be processed (e.g. collected and further used) if:

The data subject has unambiguously given his or her consent, i.e. if he or she as agreed freely and specifically after being adequately informed;

Data processing is necessary for the performance of a contract involving the data subject or in order to enter into a contract requested by the data subject, e.g. processing of data for billing purposes or processing of data relating to an applicant for a job or for a loan;

Processing is required by a legal obligation;

Processing of data is necessary to protect an interest that is essential for the data subjects life. An example is in the case of a car accident and the data subject is unconscious, emergency paramedics are allowed to give blood tests if it is deemed essential to save the data subject's life;

Processing is necessary to perform tasks of public interests or tasks carried out by official authorities (such as the government, the tax authorities, the police etc.);

Finally data can be processed whenever the controller or a third party has a legitimate interest in doing so. However, this interest cannot override the interests or fundamental rights of the data subject, particularly the right to privacy. This provision establishes the need to strike a reasonable balance, in practice, between the business interest of the data controllers and the privacy of data subjects. This balance is first evaluated by the data controllers under the supervision of the data protection authorities, although if required, the courts have the final decision.

WOMBLE CARLYLE

Individual Rights

Data subjects' individual rights, as established by the Directive, are:

the right to know who the data controller is, the recipient of the data and the purpose of the processing;

the right to have inaccurate data rectified;

a right of recourse in the event of unlawful processing; and

the right to withhold permission to use data in some circumstances. For example, individuals have the right to opt-out free of charge from receiving direct marketing material.

Sensitive Personal Data

- sensitive personal data: religious beliefs, political opinions, health, sexual orientation, race, membership of past organizations.
- extra restrictions apply to processing this data. (art. 8) Only used as follows:
  - data subject's explicit consent to process sensitive data,
  - the processing of data mandated by employment law, where it may be impossible for the data subject to consent,
  - processing of data has been publicly announced by the data subject or
  - processing of data about members by trade unions, political parties or churches.

WOMBLE CARLYLE

Member States Could Add Restrictions

E.g., Germany: Worker's Circles must approve of employment data sent over seas

WOMBLE CARLYLE

US Approach

- Sectoral
  - Health care
  - Finance
  - Education
  - Children
  - Video Rentals

US Approach

- Reactive State Laws
  - Report breaches
  - Data security requirements

WOMBLE CARLYLE

The Safe Harbor Mechanism

US privacy and data protection laws were considered by us Europeans to be complex and because the US adopted a sectoral approach which relied on a mix of legislation, regulation and self-regulation, the Article 29 Working Party (EU DP Supervision) held that this approach could not be relied upon to provide an adequate level of protection. This created a real headache for International Commerce. So there had to be a "workaround" and helpfully Directive 95/46 provides that the Commission can decide a third country has adequate levels of protection where domestic law or commitments ensures this.

The EU Privacy Commission issued Decision 2000/520 which authorises the transfer of personal data from Europe to undertakings in the US which have undertaken to comply with the Safe Harbor principles.

WOMBLE CARLYLE

What was the Safe Harbor Mechanism?

US companies storing customer data may self-certify that they adhere to 7 principles, to comply with the EU Data Protection Directive and with Swiss requirements.

The Safe Harbor mechanism was an agreed benchmark/a set of standards which for when adhered to would protect the rights of Europeans when their personal data was being transferred to signatories of the Scheme in the USA.

And critically was recognised under decision 2000/520 of the European Commission providing adequate protection for data transferred from the EU to the USA.

WOMBLE CARLYLE

The Safe Harbor Mechanism

That protection arose from the implementation of and adherence to a set of 7 Safe Harbor Principles (found in Annex I to Decision 520) and the related FAQ's issued by the US Dept. of Commerce (found in Annex II to Decision 520) which provided guidance on the implementation of the 7 principles.

Those 7 principles are broadly related to the principles under which European Data Protection laws are currently derived from under Directive 95/46.

The Safe Harbor Mechanism

Directive 95/46 contains a number of rules on the transfer of personal data to non EU countries.

And Article 25 states that the transfer to a non EU country of personal data which is or will be processed after transfer may only take place if that third country ensures an adequate level of protection of such data which is equivalent to Europe.

WOMBLE CARLYLE

How did the Safe Harbor Operate?

A voluntary program signing up to the principles participation meant publicly declaring your participation and self-certifying on an annual basis your organizations compliance.

Seen by many in Europe as not particularly onerous.

WOMBLE CARLYLE

Enforcement of the Safe Harbor

The FTC has the authority to take action where unfair or deceptive acts or practices in or affecting commerce take place. Companies in having to self-certify that they will protect the information they collect in accordance with Safe Harbor principles, where it failed to do so, then this would be a misrepresentation and a deceptive practice for the purposes of Section 5 of the FTCA.

The Dept. of Commerce was to review self-certification and every annual re-certification from companies to ensure that they included all elements required to be a member of the Scheme. It also kept and published an up-to-date list of the companies.

10 Things I Hate About You

- Basic Approach with no objective protections
- Private Issues
  - Google
  - Facebook
  - Data Aggregators
- Public Issues
  - Lacking enforcement of safe harbor
  - USA PATRIOT Act
  - Snowdon Revelations

WOMBLE CARLYLE

Enforcement in Reality

- Very little FTC attention paid for many years
  - First 10 year – 0 complaints so no enforcement actions.
  - 2009 to 2013 the FTC brought a total of 10 enforcement actions.
  - In 2013 there were 3246 certified companies, making the enforcement rate 0.3%.
  - 2014 enforcements against 12 U.S. companies, 15 actions in 2015.

WOMBLE CARLYLE

EU Frustrations Boil Over Into

- Right to be forgotten
- Google Executive Prosecution
- Schrems case (removing safe harbor)

WOMBLE CARLYLE

Max Schrems v. Irish Data Protection Commissioner

The Court of Justice of the European Union (CJEU) issued the final ruling in Schrems v. Data Protection Commissioner (Case C-362/14) on October 6, 2015, invalidating the Safe Harbor arrangement.

WOMBLE CARLYLE

Schrems Case

- Max Schrems, an Austrian law student and privacy advocate, has been a Facebook user since 2008. Some or all of the data provided by Mr. Schrems to Facebook is transferred from Facebook's Irish subsidiary to servers located in the United States and held there.
- Mr. Schrems lodged a complaint with the Irish data protection authority (the Data Protection Commissioner), taking the view that, in the light of the revelations made in 2013 by Edward Snowden concerning the activities of the United States intelligence services (in particular the National Security Agency 'the NSA'), the law and practices of the United States offer no real protection against surveillance by the United States of the data transferred to that country.

WOMBLE CARLYLE

Schrems Case

- The Irish authority rejected the complaint, holding that in a July 26, 2000 decision the EU Privacy Commission considered that, under the 'safe harbor' scheme, the United States ensures an adequate level of protection of the personal data transferred.
- Mr. Schrems appealed the decision of the Data Protection Commissioner before the Irish High Court. The Court decided to stay the proceedings and to refer questions to the European Court of Justice on the specific query:
  - May and/or must the national data protection supervisory authority conduct his or her own investigation of the adequacy of data protection in a third country or the Commissioner is absolutely bound by the Commission's decision?

Schrems Case: AG Opinion

On September 23, 2015, Advocate General Yves Bot issued his opinion that the Safe Harbor arrangement, which permits the transfer of personal data from the EU to the US without legal protection, must end because the arrangement fails to protect privacy and "must be declared invalid."

Schrems Ruling
October 6, 2015

"The Court of Justice holds that the existence of a Commission decision finding that a third country ensures an adequate level of protection of the personal data transferred cannot eliminate or even reduce the powers available to the national supervisory authorities under the Charter of Fundamental Rights of the European Union and the directive. **It is thus ultimately the Court of Justice which has the task of deciding whether or not a Commission decision is valid.** "

WOMBLE CARLYLE

Schrems Ruling
October 6, 2015

"The Court observes that … United States public authorities are not themselves subject to [the safe harbor regime]. Furthermore, national security, public interest and law enforcement requirements of the United States prevail over the safe harbor scheme, so that United States undertakings are bound to disregard, without limitation, the protective rules laid down by that scheme where they conflict with such requirements."

WOMBLE CARLYLE

Schrems Ruling
October 6, 2015

"United States authorities were able to access the personal data transferred from [EU} Member States to the United States and process it in a way incompatible, in particular, with the purposes for which it was transferred, beyond what was strictly necessary and proportionate to the protection of national security. Also, the Commission noted that the persons concerned had **no administrative or judicial means of redress** enabling, in particular, the data relating to them to be accessed and, as the case may be, rectified or erased."

WOMBLE CARLYLE

Completely Illogical

- Making business suffer for government actions
- EU member states do the SAME things – see new French surveillance rule
- This logic disqualifies all means of business protecting data (contract terms)
- There are other clear reasons to strike safe harbor that could have been cited (enforcement)

WOMBLE CARLYLE

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

- ALTERNATIVE BASES FOR TRANSFERS OF PERSONAL DATA TO THE U.S
- The Commission will now draw the necessary consequences from the judgment by shortly preparing a decision, to be adopted pursuant to the applicable comitology procedure, replacing that provision in all existing adequacy decisions.

WOMBLE CARLYLE

Current Regime

- Companies that have switched to other protections will not face enforcement.
- Less certainty for those relying on safe harbor
- While some DPAs threatened to block transfers, all are taking a common position now

WOMBLE CARLYLE

New Deal

Four Primary Rules:

- processing must be based on “clear, precise and accessible rules”
- there should be “necessity and proportionality” in accessing personal data from European citizens
- there needs to be an independent oversight mechanism to oversee how EU citizens’ data is being accessed by intelligence services
- there must be “effective remedies” open to EU individuals wanting to make complaints — “and anyone should have right to defend her/his right before an independent body”

WOMBLE CARLYLE

Privacy Shield Includes

Strong obligations on companies handling Europeans' personal data and robust enforcement: U.S. companies wishing to import personal data from Europe will need to commit to robust obligations on how personal data is processed and individual rights are guaranteed. The Department of Commerce will monitor that companies publish their commitments, which makes them enforceable under U.S. law by the US. Federal Trade Commission. In addition, any company handling human resources data from Europe has to commit to comply with decisions by European DPAs.

WOMBLE CARLYLE

Privacy Shield Includes

Clear safeguards and transparency obligations on U.S. government access: For the first time, the US has given the EU written assurances that the access of public authorities for law enforcement and national security will be subject to clear limitations, safeguards and oversight mechanisms. These exceptions must be used only to the extent necessary and proportionate. The U.S. has ruled out indiscriminate mass surveillance on the personal data transferred to the US under the new arrangement. To regularly monitor the functioning of the arrangement there will be an annual joint review, which will also include the issue of national security access. The European Commission and the U.S. Department of Commerce will conduct the review and invite national intelligence experts from the U.S. and European Data Protection Authorities to it.

WOMBLE CARLYLE

Privacy Shield Includes

Effective protection of EU citizens' rights with several redress possibilities: Any citizen who considers that their data has been misused under the new arrangement will have several redress possibilities. Companies have deadlines to reply to complaints. European DPAs can refer complaints to the Department of Commerce and the Federal Trade Commission. In addition, Alternative Dispute resolution will be free of charge. For complaints on possible access by national intelligence authorities, a new Ombudsperson will be created.

Privacy Shield Includes

Considerably more work in enforcement by U.S. Agencies

Detailed Self-Certification

New Arbitration Procedures

Companies Subject to Audits

Liability and Sanctions (sufficiently rigorous to ensure compliance)

WOMBLE CARLYLE

Privacy Shield Includes

Right to be forgotten by companies

Right of Access for Data

DPA Panels to "give advice" to U.S. Companies

Booted off List for Consistent Noncompliance

WOMBLE CARLYLE

New Deal

Privacy Shield arrangement includes exceptions to allow for some US mass surveillance of EU citizens data — EU Commissioner Vera Jourová listing three circumstances when "generalized access" would be allowed: "if the tailored and targeted access is not technically or operationally possible; or if they see some very dangerous trend that needs more than targeted access"

WOMBLE CARLYLE

Harvard Business Review

"There's more than a whiff of hypocrisy here, suggesting once again that the privacy red flag is being waved more to hamstring U.S. tech giants than to protect EU citizens. It's all part of last year's Digital Single Market initiative in the EU, which, despite its name, has so far been more about erecting protectionist trade barriers than solving Europe's innovation deficit. (The EU is also ramping up wide-ranging antitrust actions against leading U.S. internet companies, for example.)

To the extent that the privacy concerns in Europe are genuine, they are a reflection of a profoundly different approach to privacy in two giant economies. U.S. privacy law, inspired by our revolutionary founding, focuses more on restrictions, such as the Fourth Amendment, that protect citizens from information collection and use by government rather than private actors. In fact, private actors are often protected from such restrictions by the First Amendment."

WOMBLE CARLYLE

Harvard Business Review

"And it's hardly clear that the EU's broad privacy directives translate to stronger protections. The rhetoric may be strong, but the EU's central government is weak, leaving enforcement to member states, whose implementations and enthusiasm vary wildly. As a result, privacy law in the EU is even more disjointed than in the U.S."

WOMBLE CARLYLE

Next Steps

The College mandated Vice-President **Ansip** and Commissioner **Jourová** to prepare a draft "adequacy decision" in the coming weeks, which could then be adopted by the College after obtaining the advice of the Article 29 Working Party and after consulting a committee composed of representatives of the Member States.

In the meantime, the U.S. side will make the necessary preparations to put in place the new framework, monitoring mechanisms and new Ombudsman.

WOMBLE CARLYLE

Article 31 Committee has Final Say

- Article 29 Working Party, European Data Protection Supervisor and European Parliament only allowed to give opinions and European Commission may not follow
- Pushing for a sunset clause
- EU wants judicial redress against the NSA

WOMBLE CARLYLE

Model Clauses no Jeopardized

- Irish DPC refers case to the ECJ
- Can Facebook use standard clauses to transfer data out of EU?

WOMBLE CARLYLE

Other Factors

- Status of the UK (Brexit)
- French insist Data Remains in EU

WOMBLE CARLYLE

Take Aways

- Business is at the mercy of our law enforcement establishment
- Expect many, many claims in the future
- Is the Genie out of the bottle?

WOMBLE CARLYLE

Thank You

Ted Claypoole

704 331-4910

tclaypoole@wcsr.com

http://www.wcsr.com/Professionals/Lawyer-Bios/Theodore-F-Claypoole

WOMBLE CARLYLE