Overview

- Comparative Approaches to Contract: US and EU
- Four Assessment Factors
- US Approach to Contractual Privacy
- EU Approach to Contractual Privacy
- The Future
The Future
Two Working Theories

• EU: strenuous efforts to protect consumers
• US: a reign of boilerplate
Four Assessment Factors

• Relevant harms
• Legal institutions for policing contractual privacy
• Kinds of enforcement mechanisms in place
• Impact of technology
U.S. Approach to Contractual Privacy

• Binding statements of practice
• Privacy federalism
• Enforcement of privacy and security statements, development of substantive requirements
• Not equivalent to EU data protection
Assessing the U.S. Approach to Contractual Privacy

• Institutions: Congress, state legislatures, FTC and state AG’s. More limited role for judges developing contract law
• Harm: US law still in search of theory of privacy harms
• Enforcement: high FTC fines
• Technology: embedded “surveillance capitalism”
EU Approach to Contractual Privacy

- Continuity: skepticism of consensual approaches
- Consent carefully embedded in legal and social structures and limited in reach
- Unwaivable data privacy interests: not alienable through contracts
GDPR on Consent, Article 7

• If consent is presented as part of written declaration that concerns other matters, “the request for consent must be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language”
• Right to withdraw consent at any time. “It shall be as easy to withdraw consent as to give it”
• “When assessing whether consent is freely given, utmost account shall be taken of the fact whether, among others, the performance of a contract, including the provision of a service, is made conditional on the consent to the processing of data that is not necessary for the performance of this contract.”
Assessing the EU Approach to Contractual Privacy

• Institutions: wide range of institutions involved— from Brussels to Member States
• Harm: well-developed law of privacy harms
• Enforcement: low fines, weak enforcement but changes under GDPR
• Technology: same “surveillance capitalism” as in US
The Future
Contracting and Privacy: Today and Tomorrow

- EU and U.S.: Future of convergence or divergence for contractual privacy?
Assessing the Future for EU and US Approaches to Contractual Privacy

- **Institutions**: US - greater role for state AG’s? EU - shift to Brussels? Privacy federalism?
- **Harm**: future divergence likely. Testing FTC enforcement of contract-lite?
- **Enforcement**: coming will be tough EU enforcement based on antitrust model
- **Technology**: Snowden marking a turning point? Technological momentum?
Facebook Faces German Antitrust Investigation

By MARK SCOTT  MARCH 2, 2016
The General Data Protection Regulation
Dr. Anna Zeiter, L.L.M
Head of Data Protection
EMEA Region
eBay, Inc.
The “One-stop-shop” Rule: Article 51

Article 51

Competence

1. Each supervisory authority shall be competent to perform the tasks and exercise the powers conferred on it in accordance with this Regulation on the territory of its own Member State.

2. Where the processing is carried out by public authorities or private bodies acting on the basis of points (c) or (e) of Article 6(1), the supervisory authority of the Member State concerned shall be competent. In such cases Article 51a does not apply.

3. Supervisory authorities shall not be competent to supervise processing operations of courts acting in their judicial capacity.
And the award for Most Misleading Title goes to…

One-stop-shop!
The “One-stop-shop” Rule
The “One-stop-shop” Rule: Article 51

Article 51

Competence

1. Each supervisory authority shall be competent to perform the tasks and exercise the powers conferred on it in accordance with this Regulation on the territory of its own Member State.

2. Where the processing is carried out by public authorities or private bodies acting on the basis of points (c) or (e) of Article 6(1), the supervisory authority of the Member State concerned shall be competent. In such cases Article 51a does not apply.

3. Supervisory authorities shall not be competent to supervise processing operations of courts acting in their judicial capacity.
James Koenig, Paul Hastings
Of Counsel, Litigation
Privacy and Cybersecurity
Practice Group
Article 17 of the GDPR: The RTBF

Article 17

Right to erasure ("right to be forgotten")

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

(a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing of the data;

(c) the data subject objects to the processing of personal data pursuant to Article 19(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing of personal data pursuant to Article 19(2);

(d) they have been unlawfully processed;

(e) the data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

(f) the data have been collected in relation to the offering of information society services referred to in Article 8(1).
The Company That Knew Too Much
The RTBF: Article 17 of the GDPR

Article 17
Right to erasure ("right to be forgotten")

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:
   
   (a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

   (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing of the data;

   (c) the data subject objects to the processing of personal data pursuant to Article 19(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing of personal data pursuant to Article 19(2);

   (d) they have been unlawfully processed;

   (e) the data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

   (f) the data have been collected in relation to the offering of information society services referred to in Article 8(1).
Prof. Dr. Karl-Nikolaus Peifer
Director,
Institute for Media Law
And Communications Law
And Director,
Institute for Broadcasting Law
University of Cologne
Jurisdiction under the GDPR: Article 3

Article 3

Territorial scope

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

(b) the monitoring of their behaviour as far as their behaviour takes place within the European Union.

3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where the national law of a Member State applies by virtue of public international law.
Article III of the GDPR: Forbidden Planet
The “data processor”: GDPR, Article 5, defined in Article 4(6)
Jurisdiction under the GDPR: Article III

Article 3

Territorial scope

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

   (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

   (b) the monitoring of their behaviour as far as their behaviour takes place within the European Union.

3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where the national law of a Member State applies by virtue of public international law.
Kurt Wimmer, Covington Partner, Chair of the Data Privacy and Cybersecurity Practice Group
The GDPR Provides for Fines of Up to 4% of Annual Worldwide Turnover

Article 79

General conditions for imposing administrative fines

1a. Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 3 (new), 3a (new), 3aa (new) shall in each individual case be effective, proportionate and dissuasive.

2. (...)

2a. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (fa) and (h) of paragraph 1b of Article 53. When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:
The Terminator

In the Year of Darkness, 2029, the rulers of this planet devised the ultimate plan. They would reshape the future by changing the past. The plan required something that felt no pity. No pain. No fear. Something unstoppable. They created THE TERMINATOR.

Hemdale Presents a Pacific Western Production of a James Cameron Film
Arnold Schwarzenegger, "The Terminator," Michael Biehn, Linda Hamilton and Paul Winfield
Make-Up Effects by Stan Winston – Executive Producers John Daly and Derek Gibson
Written by James Cameron with Gale Anne Hurd – Produced by Gale Anne Hurd

Directed by James Cameron – Prints by Deluxe

© 1984 COLUMBIA PICTURES INDUSTRIES, INC. All rights reserved.
The GDPR Provides for Fines of Up to 4% of Annual Worldwide Turnover

Article 79

General conditions for imposing administrative fines

1a. Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 3 (new), 3a (new), 3aa (new) shall in each individual case be effective, proportionate and dissuasive.

2. (...)

2a. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (fa) and (h) of paragraph 1b of Article 53. When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:
Question and Answer Period