Privacy and Information Security Law

Elizabeth Ortmann-Vincenzo

CLASS 12

Financial Data pt. 1;
International Privacy Law pt. 1

Financial Data pt. 2

2

B. THE GRAMM-LEACH-BLILEY ACT

3

Gramm-Leach-Bliley

- Allows for sharing of personal information by financial institutions
- Only protects financial information that is not public
- Affiliates of the organization can share personal information by telling customers with a general disclosure policy

4

Sharing with Nonaffiliated Companies

- Financial institutions can share personal information with nonaffiliated companies for broad purposes if individuals are provided an opportunity to first opt out

5

Security Program

- "According to the regulations, financial institutions 'shall develop, implement, and maintain a comprehensive information security program' that is appropriate to the 'size and complexity' of the institution, the 'nature and scope' of the institution's activities, and the 'sensitivity of any customer information at issue.' 16 C.F.R. §314.3(a). An '**information security program**' is defined as 'the administrative, technical, or physical safeguards [an institution uses] to access, collect, distribute, process, store, use, transmit, dispose of, or otherwise handle customer information.' §314.2(b)."

6

Preemption

- "GLBA does not preempt states laws that provider greater protection to privacy."

7

GLBA Summary

1. Financial institutions are required to establish and implement procedures keeping nonpublic personal information confidential and protecting the information from unauthorized use;
2. Customers must receive an annual notice detailing how nonpublic personal information is protection and on what basis information is shared;
3. Customers must be given the right, though not absolute, to opt-out of information sharing;

8

GLBA Summary

4. Fraudulently obtaining or using nonpublic personal information is a federal crime;
5. While the courts are split, states may not regulate the sharing of information included in the definition of consumer report contained in the FCRA;
6. A financial institution, despite GLBA restrictions, is expected to respond to information requests made as part of the judicial process.

Privacy Law in a Nutshell, 2nd Edition

9

C. FEDERAL AND STATE FINANCIAL PRIVACY LAWS

10

Bank Secrecy Act

- "Regulations promulgated under the Act by the Secretary of the Treasury require reporting to the government of financial transactions exceeding $10,000 if made within the United States and exceeding $5,000 if into or out of the United States."

11

Identity Theft Assumption and Deterrence Act

- "The Act makes it a federal crime to 'knowingly transfer or use, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law.' 18 U.S.C. §1028."

12

Actions Against Credit Card Companies

- "With the alarming increase in identity theft in recent years, commercial banks and credit card issuers have become the first, and often last, line of defense in preventing the devastating damage that identity theft inflicts. Because the injury resulting from the negligent issuance of a credit card is foreseeable and preventable, the Court finds that under Tennessee negligence law, **Defendant has a duty to verify the authenticity and accuracy of a credit account application before issuing a credit card**. The Court, however, emphasizes that this duty to verify does not impose upon Defendant a duty to prevent all identity theft."
- Wolfe v. MBNA America Bank

13

International Privacy Law pt. 1

14

International Privacy Law

- Europe – omnibus privacy law
  - Focus on privacy as a human right
- US – sectoral privacy laws

15

Organization for Economic Cooperation and Development (OECD)

- 34 member countries including US
- Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (the Guidelines) of 1980
  - Guidelines "establish eight key principles for the protection of personal information. It creates a non-binding framework that is intended to influence policymaking about privacy throughout the world."

16

Personal Data under OECD

- "Personal data" is defined as "any information relating to an identified or identifiable individual (data subject)."

17

8 Principles

1) Collection Limitation
2) Data Quality
3) Purpose Specification
4) Use Limitation
5) Security Safeguards
6) Openness
7) Individual Participation
8) Accountability

18

Self-Regulation and International Data Flow

- Guidelines stress self-regulation
  - "A Member country should refrain from restricting transborder flows of personal data between itself and another Member country except where the latter does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation."

19

2013 Guidelines

- 2013 guidelines update but do not replace previous guidelines
- Establishment of privacy enforcement authorities

20

B. PRIVACY PROTECTION IN EUROPE

21

European Convention on Human Rights

- “[W]as intended to bring violations of human rights to the attention of the international community.”
- “The Court’s judgment is binding upon the member state against which the application was brought.”

22

ECHR Article 8

Article 8 — Right to Respect for Private and Family Life

1.Everyone has the right to respect for his private and family life, his home and his correspondence.

2.There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

23

EU Charter of Fundamental Rights – Article 7

- Everyone has the right to respect for his or her private and family life, home and communications.

24

EU Charter of Fundamental Rights – Article 8

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

25

European Union Data Protection Directive

- "The European Union Data Protection Directive of 1995 **establishes common rules for data protection among Member States of the European Union**. The Directive was created in the early 1990s and formally adopted in 1995. The EU is now in the process of replacing it with a General Regulation on Data Protection (Proposed Regulation). The Commission introduced the Proposed Regulation in 2012, and the Parliament passed an amended version of it in 2014. Once enacted, the Proposed Regulation will replace the Directive and be directly binding on all Member States."

26

EU Data Protection Directive: Implementation of Directives

- "Directives are a form of EU law that is **binding for Member States**, but **only as to the result** to be achieved. They allow the national authorities to choose the form and the methods of their implementation and generally fix a deadline for it. Therefore, the rules of law applicable in each Member State are the national laws implementing the directives and not the directive itself. However, the directive has a 'direct effect' on individuals: **it grants them rights that can be upheld by the national courts in their respective countries if their governments have not implemented the directive** by the set deadline. A directive thus grants *rights* rather than creates obligations, and they are enforceable by *individuals* rather than by public authorities."

27

EU Data Protection Directive: Controlled Data Usage

- "The Directive also gives individuals substantial **rights to control the use of data about themselves**. These rights include the right to be **informed** that their personal data are being transferred, the need to obtain '**unambiguous' consent** from the individual for the transfer of certain data, the opportunity to **make corrections** in the data, and the **right to object to the transfer**."

28

EU Data Protection Directive: Article 25

- "The Directive extends privacy safeguards to personal data that are transferred outside of the European Union. Article 25 of the Directive states that data can only be transferred to third countries that provide an 'adequate level of data protection.' As a result, implementation focuses on both the adoption of national law within the European Union and the adoption of adequate methods for privacy protection in third party countries."

29

EU Data Protection Directive: Article 2 Definitions

- (a) "**personal data**" shall mean 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;
- (b) "**processing of personal data**" ("processing") shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

30

EU Data Protection Directive: Article 2 Definitions

- (c) "**personal data filing system**" ("filing system") shall mean any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;
- (d) "**controller**" shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;
- (e) "**processor**" shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

31

EU Data Protection Directive: Article 2 Definitions

- (f) "**third party**" shall mean any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data;
- (g) "**recipient**" shall mean a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients;
- (h) "**the data subject's consent**" shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

32

EU Data Protection Directive: Notification Requirement

- "Obligation to Notify the Supervisory Authority. Under Article 18, the '**controller**' (the entity determining the purposes of the data processing) **must notify the 'supervisory authority' before carrying out any partly or wholly automatic processing operation**. If certain conditions are met, Member States may enact rules exempting controllers from notifying the supervisory authority (or simplifying the notification)."

33

EU Data Protection Directive: European Data Protection Supervisor (EDPS)

- "In 2001, the European Community promulgated Regulation No. 45/2001, which established data protection rules for the processing of personal data by Community institutions. This regulation also established the **European Data Protection Supervisor (EDPS) as an independent supervisory authority with responsibility for monitoring the processing of personal data by Community institutions**. The EDPS has a further role in advising European institutions and national supervisory authorities on new legislation, new technology, and international developments. Finally, the EDPS has legal authority to intervene in actions before the European Court of Justice."

34

EU Data Protection Directive: International Data Transfers

- Cross-border information flow v. individual privacy
- "**Article 25** governs when Member States may permit the flow of personal data to other countries. This provision has particular relevance for the United States, because it **governs the level of privacy protections other countries must have in place for data transfers to occur**".

35

EU Data Protection Directive: Article 7

- Processing restrictions
  - Explicit consent
  - Performance of or entry into a contract
  - Compliance with a legal obligation
  - Protection of vital interests
  - Public interest or exercise of official duties
  - Balancing of the legitimate interests of controller

36

EU Data Protection Directive Article 25(1)

- The Member States shall provide that the **transfer to a third country of personal data** which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, **the third country in question ensures an adequate level of protection**.

37

EU Data Protection Directive Article 25(2)

- The **adequacy of the level of protection** afforded by a third country **shall be assessed in the light of all the circumstances surrounding a data transfer** operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.

38

EU Data Protection Directive: Derogations/Exceptions

- "Transfers of personal data to a third-party country that does not ensure an adequate level of protection under Article 25(2) may still take place on condition that the **data subject has unambiguously consented, the transfer of data is 'necessary in order to protect the vital interests of the data subject,' or the transfer serves 'important public interest grounds.'** There are several additional exceptions.
- A Member State may also authorize transfers of personal data to third countries without an adequate level of protection where protection of the privacy and individual freedoms 'result **from appropriate contractual clauses**.'"

39

EU Data Protection Directive Blocking

- "Pursuant to Article 25 of the EU Directive, transfers of personal data about European citizens can be blocked if third party countries (such as the United States) do not provide 'an adequate level of protection.'"
- "The European Directive requires the national supervisory authorities in each of the Member States and the European Commission to make comparisons between European data protection principles and foreign standards of fair information practice. The European Directive further requires that **foreign standards of fair information practice be 'adequate' in order to permit transfers of personal information** to the foreign destination."

40

EU Data Protection Directive Data Transfer outside EU

Derogations / Exceptions:

- Binding Corporate Rules
- Consent
- Standard Contract Clauses (SCCs)
- Privacy Shield (replaced Safe Harbor)

41

EU Data Protection Directive: Binding Corporate Rules

Derogation 1 of 4: BCRs

- Internal rules (such as a Code of Conduct) adopted by multinational group of companies which define global on international transfers of personal data within the same corporate group to entities located in countries which do not provide an adequate level of protection
- General Requirements:
  - Privacy principles (transparency, data quality, security, etc.),
  - Tools of effectiveness (audit, training, complaint handling system, etc.),
  - And an element proving that BCR are binding.

42

EU Data Protection Directive: Consent

Derogation 2 of 4: Consent of Data Subject

- Consent must be a clear and unambiguous indication of wishes, given freely, specific and informed.
- Very high threshold

43

EU Data Protection Directive: Standard Contract Clauses

Derogation 3 of 4: SCCs

- Model contracts containing required provisions between a data exporter and data importer
- Appendices available for limited customization

44

EU Data Protection Directive: Safe Harbor

- Derogation 4 of 4
- July 2000 agreement between the U.S. Department of Commerce and EU Commission to formulate **a 'safe harbor' agreement to ensure that the United States met the EU Data Directive's 'adequacy' requirement in Article 25**.
  - Comply with safe harbor privacy principles and FAQs
  - Publicly disclose privacy policies
  - Subject to FTC (or other gov't org) for compliance enforcement

45

EU Data Protection Directive: Schrems v Data Protection Commissioner

Challenge to Derogation 4, Safe Harbor

- Office of Advocate General
- September 2015
- Challenge to Safe Harbor validity **as a legal basis for the transfer of personal data from the European Union to undertakings established in the United States**

46

Schrems v Data Protection Commissioner

- Nature of complaint
  - Schrems is an Austrian national who uses FB
  - FB Ireland users servers based in the US
  - US offers no real protection against State surveillance (as shown after Snowden revelations)

47

Schrems Case Timeline

- 6/25/13 – Complaint filed to Irish Data Protection Authority by Schrems
- 6/18/14 – Irish high court refers complaint to the European Court of Justice (RCJ)
- 9/23/15 – AG opinion suggests the safe harbor invalid [per slides above]
- 10/6/15 – Court of Justice of the European Union (CJEU) invalidates the safe harbor [per slide below]

48

Schrems Case: Court of Justice of the EU

- Decision 2000/520 is invalid.
- Supervisory authority of member state can examine a claim "concerning the protection of his rights and freedoms in regard to the processing of personal data relating to him which has been transferred from a Member State to that third country when that person contends that the law and practices in force in the third country do not ensure an adequate level of protection."

49

EU Data Protection Directive: Privacy Shield

- "Safe Harbor 2.0"
- The EU-U.S. Privacy Shield Framework was designed by the U.S. Department of Commerce and European Commission to provide companies on both sides of the Atlantic with a mechanism to comply with EU data protection requirements when transferring personal data from the European Union to the United States in support of transatlantic commerce.

50

EU Data Protection Directive: Privacy Shield

- Effective July 12, 2016
- Self Certification Program
- Article 29 Working Party acceptance was key
- Approx. 500 companies currently self certified

51

EU Data Protection Directive: Privacy Shield

Privacy Shield Principles

1. Notice
2. Choice
3. Accountability for Onward Transfer
4. Security
5. Data Integrity and Purpose Limitation
6. Access
7. Recourse, Enforcement and Liability

52

EU Data Protection Directive: Privacy Shield

Privacy Shield Supplemental Principles:

- Sensitive Data; Journalistic Exceptions; Secondary Liability; Performing Due Diligence and Conducting Audits; The Role of the Data Protection Authorities; Self-Certification; Verification; Access; Human Resources Data; Obligatory Contracts for Onward Transfers; Dispute Resolution and Enforcement; Choice – Timing of Opt-Out; Travel Information; Pharmaceutical and Medical Products; Public Record and Publicly Available Information; Access Requests by Public Authorities
- Legal Challenge filed Nov. 1

53

European Union General Data Protection Directive

The European Union Data Protection Directive of 1995 **establishes common rules for data protection among Member States of the European Union**. The Directive was created in the early 1990s and formally adopted in 1995. The EU is now in the process of replacing it with a General Regulation on Data Protection, which will take effect on May 25, 2018.

54

European Union General Data Protection Directive

- Replaces Data Protection Directive
- Attempts to harmonize country-specific differences that were the result of the DPD
- Many similar concepts as DPD, but significantly higher standards
- More sophisticated on technology

55

GDPR: Highlights & Key Differences from DPD

- Increased Enforcement: Max fines quadruple
- Harmonization: Unlike the DPD, no need for country specific implementation, which will result in greater consistency
- Expanded Territorial Scope
- Consent harder to obtain

56

GDPR: Highlights & Key Differences from DPD

- Risk-Based Approach is available
- One Stop Shop of lead Data Protection Authority
- Data Protection by design and by default
- Comprehensive data protection compliance program is required, with policies, procedures and compliance infrastructure

57

GDPR: Highlights & Key Differences from DPD

- Heightened obligations on processors
- Stricter data breach notification requirements
- Pseudonymization
- BCR

58

GDPR: Highlights & Key Differences from DPD

- The Right to Be Forgotten
- The Right to Object to Profiling
- The Right to Data Portability

59

Program Completed

60