

PRIVACY IN THE NEW WORLD ORDER

Part I
Compliance (2017)

Part II
Globalization (2018)



Part III
The Age of Turmoil
(April, 2020)

Part IV
The Privacy Shield Falls
(December, 2020)

Series Presented in Collaboration with
Thomson Reuters

Privacy in the New World Order

CONTINUING LEGAL EDUCATION THOMSON REUTERS

Sapronov & Associates, P.C.
1200 Abernathy Road, Suite 1700
Atlanta, Georgia 30346
www.wstelecomlaw.com
(770) 399-9100



Privacy in the New World Order

Part 1: Compliance

2

- Introduction
- Privacy Compliance in the U.S.
- Privacy Compliance in the E.U.
- The FCC's New Privacy Rules
- The U.S. Election: Upheaval Begins

INTRODUCTION

- Privacy in the New World Order:
 - Characterized by Aggressive Enforcement of Privacy Laws
 - Both in the U.S. and European Union (EU)
 - U.S. - Multi-jurisdictional privacy enforcement
 - Federal Communications Commission (FCC)
 - Federal Trade Commission (FTC)
 - State Attorneys General
 - EU - Demise of “Safe Harbor” for EU-U.S. Cross-border privacy protections and new regulation
 - Replaced by “Privacy Shield”
 - And future General Data Protection Regulation (GDPR)
 - FCC Privacy Order is latest example of this trend

INTRODUCTION (*Cont.*)

4

- Privacy in the New World Order: (*cont'd*)
 - Privacy enforcement can trigger severe penalties
 - FCC forfeiture and penalty assessment
 - FTC disgorgement penalties and injunctions
 - Federal and state “Do not contact” laws – Statutory penalties
 - State actions – *e.g.*, Data breach notification laws
 - Private Causes of Action
 - Communications Act
 - Electronic Communications Privacy Act
 - Telephone Consumer Protection Act (TCPA)
 - Data breach (class action, tort claims, shareholder suits)
 - EU: GDPR violation – up to 4 % of Global Revenues

Privacy Compliance in the United States

5

- Generally
 - Recent proliferation of enforcement actions by U.S. federal and state authorities
 - Especially for privacy, data breach and “Do not contact” violations
- Authority found in:
 - Federal Communications Act (Title 47 U.S.C. §151 et. seq.)
 - Federal Trade Commission Act (15 U.S.C. §§41-58)
- Enforced by the Federal Communications Commission (FCC) and Federal Trade Commission (FTC), respectively

Privacy Compliance in the United States (cont'd)

6

- Historically, FCC regulated privacy of customers' information under "CPNI" statute
 - (47 U.S.C. § 222) and related rules
 - Applicable to telecommunications (common carriers) under "Title II" of Communications Act

- Recently, FCC privacy enforcement authority was expanded by:
 - Open Internet ("Net Neutrality") Order
 - Reclassification of BIAS Providers as Common Carriers Under "Title II" of Communications Act
 - Adoption of new privacy rules applicable thereto

Privacy Compliance in the United States (*Cont.*)

7

- FCC and FTC released Memorandum of Understanding (MOU) on 11/16/2015
 - Announcing cooperation in consumer protection (*e.g.*, privacy matters)
 - Telecommunications carriers largely exempt from FTC authority under FTC Act
 - MOU intended to close this “loophole”
 - But exemption remains complicated with reclassification of BIAS under Title II
 - and thus arguably exempt from FTC jurisdiction
 - While degree of agency enforcement under new administration remains to be seen

Privacy Compliance in the United States (*Cont.*)

8

➤ Data Breach Notification Laws

➤ FTC had also expanded its privacy enforcement actions to include companies' liability for failure to protect consumer data from cyber-attacks

➤ *FTC v. Wyndham Worldwide Corporation*, August, 2015
(Third Circuit Court of Appeals affirming FTC jurisdiction to regulate hotel operator's cybersecurity practices as unfair practice)

➤ New FCC Privacy Rules (see below) also treat data breach as privacy violation

Privacy Compliance in the United States (*Cont.*)

9

- Data Breach Notification and other State Privacy Laws.
 - ❖ Codified on a multi-state basis
 - ❖ Typically trigger notice requirements upon discovery of data breach that compromises personal information (*e.g.*, Home Depot, Target)
 - ❖ State privacy laws enforced by attorneys general

Privacy Compliance in the United States (*Cont.*)

10

- “Do Not Contact” Laws
 - ❖ Multi-jurisdictional enforcement under Telephone Consumer Protection Act (TCPA), FTC Act (“Sales rule”); and multi-state “do not call” regulations
 - ❖ Recent appeals of expansive TCPA enforcement by FCC have surfaced but both government and private actions continue
 - ❖ Legislative review pending but full rewrite unlikely

Privacy Compliance in the EU

11

- Generally
 - ❖ Comprehensive framework and ‘harmonized’
 - ❖ Impact of Maximilian Schremms v Data Protection Commissioner
 - ❖ EU Safe Harbor 2.0 (Privacy Shield)
 - ❖ General Data Protection Regulation (GDPR)
 - ❖ New ePrivacy regulation on the horizon
 - ❖ EU Data Protection Authority Enforcement

Privacy Compliance in the EU (*Cont.*)

12

- Cross-border transfers: transfer at your own risk
 - ❖ Invalidation of Safe Harbor
 - ❖ Cross-border contracts vulnerable
 - ❖ Model Clauses v. Binding Corporate Rules
 - ❖ BCR and the GDPR

Privacy Compliance in the EU (*Cont.*)

13

- Some key changes under the GDPR
 - ❖ Better harmonization (or not?)
 - ❖ Principle of accountability
 - ❖ Increased sanctions
 - ❖ Data breach notifications
 - ❖ Privacy by Design / Privacy Impact Assessments

Privacy Compliance in the EU (*Cont.*)

14

- Looking forward to GDPR readiness
 - ❖ DPO (obligatory?)
 - ❖ Lead Data Protection Authority: how to determine main establishment?
 - ❖ Processor responsibility
 - ❖ Recent WP 29 guidance: data portability, DPO and main establishment
 - ❖ Class actions now on the horizon?
 - ❖ Getting an early start: the case of France
 - ❖ Time to prepare is now: audits, resourcing, training, processes...

The FCC's New Privacy Rules

15

- The FCC's New Privacy Rules:
 - Long anticipated, released Nov. 2, 2016
 - Revisions announced in FCC Open Internet (Net Neutrality) Order
 - Privacy Order revises and expands current privacy rules applicable to telecommunications carriers
 - Specifically targets Broadband Internet Access Providers (“BIAS”), not just traditional carriers
 - And broadly expands protected content to include:
 - Customer Proprietary Network Information (“CPNI”) and
 - Personally Identifiable Information (“PII”) - Into
 - New category: Personal Information” (“PI”)

The FCC's New Privacy Rules (continued)

16

- New FCC Privacy Rules:
 - Codified in scattered sections of 47 C.F.R. Part 64
 - Order adopted and Rules Published shortly after U.S. election – (Dec. 3, 2016)
 - Effective date of rules varies (some as early as January, 2017)
 - Whether they survive change in U.S. Administration remains to be seen
 - But for now have the effect of law

The U.S. Election: Upheaval Begins

17

- Privacy in the New World Order:
 - Upheaval Begins with U.S. Presidential Election
 - Republican sweep causes administrative uncertainty
 - Little known of President Elect's telecommunications policies
 - Other than Opposition to Net Neutrality
 - FCC Open Internet Order is basis of FCC Privacy Rules
 - Likely opposition to Privacy Rules can be inferred

The U.S. Election: Upheaval Begins (*Cont.*)

18

- Other Possible Challenges to FCC Privacy Rules
 - Congressional Review Act of 1996
 - 60 Day Congressional Review of Federal Regulations
 - Regulations subject to Congressional Resolution of Disapproval
 - President can Veto, so relatively ineffective
 - Until Now!

CONCLUSION

- More changes certain to follow with new U.S. Administration
- For now, much uncertainty
- New developments and liability issues to be discussed in Parts II and III of this program (stay tuned)

CONCLUSION

20

All of this is very complicated ...

**BUT... DO REMEMBER:
WHEN IN DOUBT – ASK YOUR LAWYER!**

**Sapronov & Associates, P.C.
1200 Abernathy Rd., Suite 1200
Atlanta, Georgia 30328
Telephone: 770-399-9100
Mobile: 770-309-0462
Facsimile: 770-395-0505
Email: info@wstelecomlaw.com
Website: www.wstelecomlaw.com**



Walt Saprnov



21

770.399.9100
wsaprnov@wstelecomlaw.com



Walt Saprnov has represented corporate clients in telecom transactions, regulation and privacy for over thirty years. He has been named in Georgia Super Lawyers and in the International Who's Who of Telecom Lawyers. Together with his Firm, Saprnov & Associates, P.C., he has negotiated commercial telecom contracts with every major telecom carrier in the U.S. and with many abroad. The Firm also supports clients in privacy compliance before the FCC, the FTC, EU and state regulatory agencies. Mr. Saprnov is a frequent conference speaker and has authored numerous publications on telecommunications law.

For more information, please visit:
www.wstelecomlaw.com

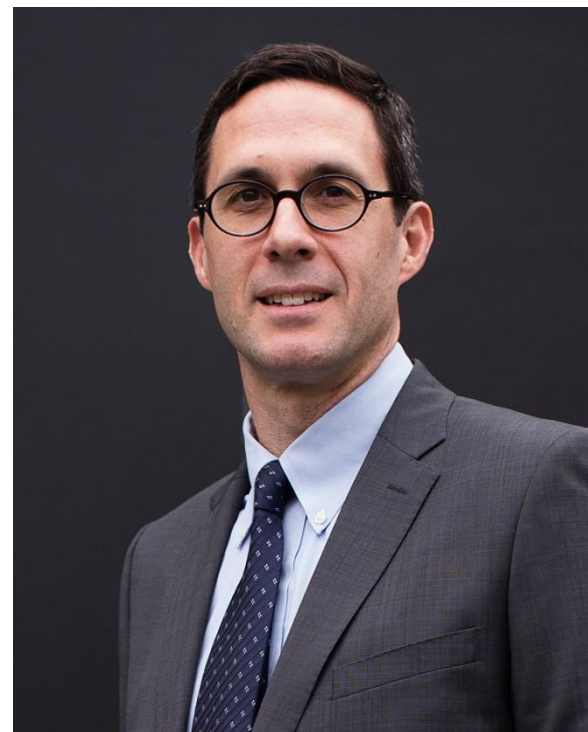
Joseph Srouji



22

Mr. Srouji, based in Paris, France, is Of Counsel to Sapronov & Associates, P.C. and Founding Partner of Srouji Avocats. He is former Senior Counsel for Data Protection & Regulatory Affairs at GE Capital where he worked for over 11 years based in Paris as a specialist in data protection, financial and banking regulation and compliance.

He teaches International Law and Technology Law to graduate students at Université Paris II Panthéon – Assas. He is a member of the Paris Bar and certified CIPP-E.



jsrouji@wstelecomlaw.com
222 Boulevard Saint Germain
75007 Paris - France
+33 (0) 1 42 60 04 31

2. Part II – Globalization (2018)

SAPRONOV & ASSOCIATES, P.C.
ATTORNEYS AT LAW

info@wstelecomlaw.com
www.wstelecomlaw.com

1200 ABERNATHY ROAD, SUITE 1700
ATLANTA, GEORGIA 30328
TEL. 770-399-9100

1875 I STREET, NW, 5TH FLOOR
WASHINGTON, D.C. 20006
TEL. 202-429-2055

A SPECIAL CLIENT ALERT¹

Privacy in the New World Order
Part II: Globalization

December 14, 2018

Continuing our collaboration with Thomson Reuters,² we are pleased to announce Part II of our “*Privacy in the New World Order*,”³ series: “*Globalization*.” This program, a live webcast, will discuss the globalization of privacy laws, both in the U.S. and abroad, and how privacy regulators have expanded their reach far beyond their jurisdictions. The discussion will address the implications of the General Data Protection Regulation (“GDPR”), its intersection with Brexit, GDPR compliance – including its change of law impact on cross-border transactions involving multi-national companies doing business in U.K. - and the new California privacy law. Here is a brief synopsis.

In a word, privacy regulators are seeking to impose their rules not only on constituents within their respective jurisdiction, but on those outside as well. Privacy enforcement efforts, regardless of their country of origin, appear to be going global.

On May 25, 2018, the GDPR went into effect. Since its enactment, debates have raged over its practical implications not only for privacy, but for jurisdictional enforcement and sovereignty as well. As an example, Italian privacy regulators have brought an action against Facebook for its allegedly misleading data practices. The tip of the iceberg, as other enforcement actions are almost certain to follow. Still more ominously for those within the GDPR’s reach is a class action lawsuit brought against Facebook by Internet Society France on November 8, 2018. Long common in the U.S., class actions for privacy violations in the EU are

¹ THIS SPECIAL CLIENT ALERT IS PROVIDED COMPLIMENTARY TO CLIENTS AND FRIENDS OF SAPRONOV & ASSOCIATES, P.C. FOR TUTORIAL PURPOSES ONLY AND IS NOT TO BE CONSTRUED AS A LEGAL OPINION OR LEGAL ADVICE. PLEASE CONTACT US AT (770) 399-9100, OR AT info@wstelecomlaw.com IF YOU HAVE SPECIFIC QUESTIONS ABOUT THIS ALERT – OR IF YOU WISH TO BE REMOVED FROM OUR MAILING LIST.

² https://westlegaledcenter.com/program_guide/course_detail.jsf?videoCourseId=100244221&ADMIN_PREVIEW=true.

³ Part I of this series, “Compliance,” is available upon request at info@wstelecomlaw.com.

a new phenomenon.⁴ If the trend continues, potential liability for multi-national companies exposed to GDPR obligations will magnify considerably.

Then there is Brexit, the looming withdrawal of the United Kingdom from the EU on March 29, 2019. As of this writing, the fate of Brexit remains uncertain as Theresa May, the beleaguered UK Prime Minister has barely survived a vote of no confidence. During this time of troubles for the UK, little attention has been paid to post-Brexit privacy enforcement – especially for those companies whose cross-border EU traffic is subject to GDPR. How UK and EU authorities could agree on a privacy framework acceptable to both (they agree on little else) if the UK were to leave the EU is a question mark.

Meanwhile, on the domestic front, in June, 2018, California legislators passed the California Consumer Privacy Act (“CCPA”). While not effective until July 2020, the bill is already being challenged – but it may also lead to a national privacy debate. Apple CEO Tim Cook publicly announced his support for EU styled privacy regulations, calling for something similar to be adopted nationally in the U.S. He also criticized Silicon Valley for maintaining a “Data Industrial Complex:” paying lip-service to privacy protections even, according to Mr. Cook, as they secretly lobby against them.⁵ California, once again, may have started a trend.

Finally, privacy issues continue to percolate their way through Congress. Silicon Valley’s Internet and social media executives have been called in front of the U.S. Senate on multiple occasions this year to testify about privacy. Following the midterm elections however, it is difficult to imagine how a fiercely divided Congress could agree on privacy legislation. And if it did, how such federal legislation would intersect with the California and EU developments is anyone’s guess.

Please join us for an in-depth discussion on these timely, complicated topics on December 17, 2018 at 9 a.m. EST. Our panel will include: Joseph Srouji, Of Counsel to Saprnov & Associates, P.C. discussing the GDPR; Kirk Nahra, Wiley Rein, LLP, discussing the California Legislation; and Kim Roberts of King & Spalding discussing Brexit and the impact on EU data privacy laws in the UK. Walt Saprnov will serve as moderator.

We hope you will join us. But if not, recordings of the discussion are available for those who cannot make the live broadcast and of course, CLE credit. For more information and to register, please visit:

http://westlegaledcenter.com/program_guide/course_detail.jsf?videoCourseId=100244221&ADMIN_PREVIEW=true

We wish all of you Merry Christmas, Happy Holidays, and a Safe and Prosperous New Year.

⁴ See, Saprnov & Srouji, “Class & Class Consciousness” Journal of Transnational Dispute Management – <https://www.transnational-dispute-management.com/article.asp?key=2416>.

⁵ E. Peker and S. Schechner, “U.S.-wide regulation could put Apple at a relative advantage compared with Facebook and Alphabet’s Google.” WSJ. Oct. 24, 2018.

Privacy in the New World Order

CONTINUING LEGAL EDUCATION THOMSON REUTERS

December 17, 2018

**Moderated by Walt Saprnov
Saprnov & Associates, P.C.
1200 Abernathy Road, Suite 1700
Atlanta, Georgia 30346
www.wstelecomlaw.com
(770) 399-9100**

Privacy in the New World Order

Part 2: Globalization*

2

- Introduction
- GDPR
- California Legislation
- Brexit

* For a copy of Part I (Compliance) of this Privacy in the New World Order series, please contact us at info@wstelecomlaw.com

INTRODUCTION

- Privacy in the New World Order:
 - Part II: Globalization
 - 2018 - 2019:
 - Privacy regulators seek to impose their rules
 - Not only within their respective jurisdiction
 - But on those outside as well
 - Privacy enforcement efforts, regardless of their country of origin, appear to be going global

INTRODUCTION (*Cont.*)

4

- Privacy in the New World Order (*cont'd*)
- EU General Data Protection Regulation (GDPR)
Developments
 - Took Effect May 25, 2018
 - Enforcement examples:
 - Facebook (warmup?)
 - Fined €10m by Italian authorities for misleading users over its data practices
 - Practical implications
 - Compliance
 - Jurisdictional reach and enforcement

INTRODUCTION (*Cont.*)

- Privacy in the New World Order (*cont'd*)
 - Domestic (State) Privacy Developments
 - California Consumer Privacy Act (“CCPA”)
 - Passed by California legislature June, 2018
 - Not effective until July 2020
 - But additional amendment expected
 - May lead to discussion of possible federal privacy legislation

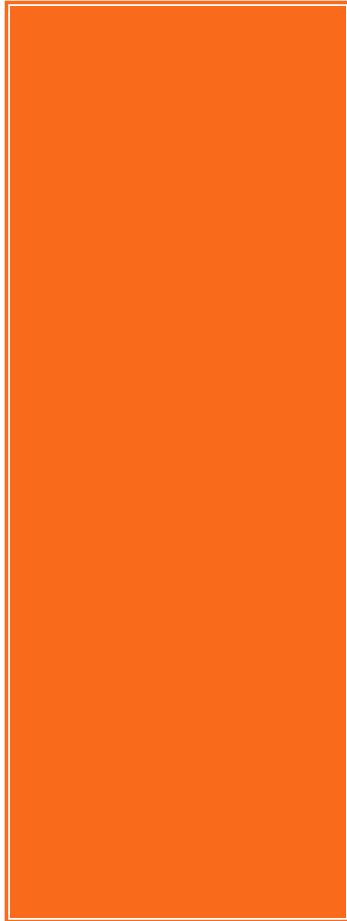
INTRODUCTION (*Cont'd*)

6

- Privacy in the New World Order (*cont'd*)
 - UK Developments
 - Anticipation of Brexit
 - Adopted by Referendum
 - UK to leave EU (March 29, 2019)
 - “Hard” or “Soft” Variations
 - Prime Minister May facing Crisis
 - Privacy Implications (among many others)
 - Consistency with GDPR
 - Recognition of UK privacy law by EU Data Protection Authorities
 - Implications for UK-EU Cross-border Transactions

EU General Data Protection Regulation (GDPR)

7



Joseph Srouji
Of Counsel
Sapronov & Associates, P.C.
215 rue du Faubourg Saint-Honore
75008 Paris – France
jsrouji@wstelecomlaw.com
+33 (0) 1 78 64 64 83

GDPR Principles

- **Reminder: main principles**
 - **Off-shore processing**
 - GDPR applies when:
 - 1) controller or processor processes personal data on EU territory;
 - 2) controller or processor is not established in the EU but processes personal data relating to persons on the EU territory.
 - **Reinforcement of data subject's rights**
 - **Transparency:** controller must give information about the process at the time of processing.
 - **Consent:** definition reinforced.
 - **New rights:** right to data portability; right to rectify, right to forget, right to limitation.
 - **Reinforced rights:** right of access; right to object.

GDPR Principles (*cont'd*)

9

- **Reminder: main principles (*cont'd*)**
 - **Accountability**
 - Principle of responsibility of the controller who must implement internal mechanisms and procedures to demonstrate compliance with data protection rules.
 - **Increased sanctioning power**
 - Supervisory authorities are vested with greater powers. They can:
 - issue a call to order;
 - order to bring the processing into compliance;
 - limit processing;
 - suspend the data flow;
 - order to comply with requests to exercise the rights of persons, including on-call duty;
 - impose an administrative fine. These fines can be up to 4% of a company's worldwide turnover.

Recap at the end of year: key figures

10

- Overview: 6 months after the entry into force of the GDPR
 - Key Figures
 - Some figures provided by the French supervisory authority, the *Commission nationale de l'informatique et des libertés* (CNIL) on the implementation of the Regulation:
 - 15,000 Data Protection Officers (DPOs) have been designated
 - More than 1000 data breach notifications have been received;
 - The CNIL website received 7 million visits
 - 130,000 simplified register model proposed by the supervisory authority have been downloaded;
 - The CNIL received 9700 complaints (34% more than in 2017 over the same period).

Examples of enforcement

11

- Overview: 4 months after the entry into force of the GDPR
- Examples of formal notices and sanctions recently imposed by the CNIL
 - Biometric Data
 - Several non-compliant practices were identified by the CNIL during an inspection at the premises of a company specializing in remote monitoring of elevators and car parks:
 - The company had set up a biometric system to monitor its employees' schedules
 - Set up a system for recording telephone calls, without informing employees
 - Workstations were not sufficiently secured
 - CNIL imposed a fine of 10,000 euros

Examples of enforcement (*cont'd*)

- Overview: 4 months after the entry into force of the GDPR
- Examples of formal notices and sanctions recently imposed by the CNIL
 - Video surveillance
 - The CNIL carried out an inspection at the premises of the “42 school,” an institution whose purpose is to train students in the field of information technology. The CNIL found :
 - Workspaces, living areas were permanently filmed by cameras
 - The people filmed were not properly informed
 - These video surveillance images were accessible in real time to all students
 - The CNIL gave notice to stop filming those areas permanently, reminded that these video images must only be accessible to authorized persons and asked the association to duly inform the persons filmed

On the horizon: class actions

13

- Group action
 - Article 80 GDPR
 - Provides that Member States may introduce into their national law the possibility of initiating a group action
 - French law:
 - Group action exists in consumer law since 2014
 - The group action in the field of personal data protection has existed since 2016 and is found in article 43 *ter* of the law
 - In practice, to launch a group action you need to have:
 - Several natural persons placed in a similar situation...
 - ...who have suffered damage due to a common cause of a similar breach
 - The event giving rise to this damage must be after 24 May 2018

On the horizon: class actions (*cont'd*)

14

- Class action
 - Current events
 - Internet Society France (ISOC) association launched a class action against Facebook on November 8, 2018
 - The association targets 7 breaches of the GDPR, including:
 - Presence of tracking cookies information about people who do not use the social network
 - Collecting sensitive data about its members (sexual orientation, political opinions, religious beliefs)
 - Cross-referencing of data between Facebook and WhatsApp without subscribers' informed consent
 - The association is claiming up to €100 million in damages

California Privacy Legislation

15

Kirk J. Nahra
Wiley Rein LLP
1776 K Street NW
Washington, DC 20006
knahra@wileyrein.com
202.719.7335



@KirkJNahrawork

California Legislation

16

- ❑ Dozens of laws dealing with privacy and security over past 15 years
- ❑ Some laws are never heard from again
- ❑ Some don't get passed elsewhere but have broader implications (*e.g.*, website privacy policies) or go national (*e.g.*, data breach, SSNs)

California Legislation

California Process

17

- ❑ Drive for referendum with aggressive privacy principles
- ❑ Industry resistance
- ❑ Last minute agreement to draft state law and agreed withdrawal of referendum proposal
- ❑ Not the normal lobbying/drafting process
- ❑ Major issue of what other states will do

California Legislation

18

- ❑ Who is protected? - “consumers” (defined as natural persons who are California residents)
- ❑ Who is covered? businesses that collect and control California residents’ personal information, do business in the State of California and: (most reasonably sized businesses - specific revenue and individual thresholds)

California Legislation Rights

19

- What rights? Four basic rights:
- (1) the right to know (through a general privacy policy and with more specifics available upon request) what personal information a business has collected about them, where it was sourced from, what it is being used for, whether it is being disclosed or sold, and to whom it is being disclosed or sold;

California Legislation Rights

20

- (2) the right to “opt out” of allowing a business to sell their personal information to third parties;
- (3) the right to have a business delete their personal information; and
- (4) the right to receive equal service and pricing from a business, even if they exercise their privacy rights under the Act.

California Legislation

21

- “Personal information” means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.
- Very broad definition, lots of variables

California Legislation

22

- Enforcement (with an opportunity to cure)
- Private right of action that allows consumers to seek statutory or actual damages and injunctive and other relief, if their sensitive personal information is subject to unauthorized access and exfiltration, theft or disclosure as a result of a business's failure to implement and maintain required reasonable security procedures. (also an opportunity to cure)

California Legislation

23

- A business shall not discriminate against a consumer because the consumer exercised any of the consumer's rights under this title.
- BUT Nothing in this subdivision prohibits a business from charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the consumer by the consumer's data.

California Legislation

- A business may offer financial incentives, including payments to consumers as compensation, for the collection of personal information, the sale of personal information, or the deletion of personal information.
- A business shall not use financial incentive practices that are unjust, unreasonable, coercive, or usurious in nature.

California Legislation Compliance Challenges

25

- Identifying California residents
- Single national approach or California specific?
- Developing operations that can adjust for those residents who exercise rights
- How does this work for vendors?

California Legislation

California & The National Debate

26

- California law has re-invigorated the national privacy debate
- Combined with GDPR and various privacy/security “problems”
- Congressional hearings
- Administration proceedings
- Stakeholders setting out their positions

California Legislation

California & The National Debate (*cont'd*)

27

- Industry is concerned about other states passing “California-like” laws
- Industry is concerned about California by itself
- Some in industry are concerned about global issues and EU “adequacy”
- Could lead to a US law – with preemption – but could be a “strong” or “weak” law

Brexit and impact on EU data privacy laws in the UK

28



Kim Roberts
King & Spalding
125 Old Broad Street
London, United Kingdom
EC2N 1AR
kroberts@kslaw.com
+44 20 7551 2133

Brexit and impact on EU data privacy laws in the UK

29

The UK is currently locked into a complex constitutional situation since the 2016 referendum resulted in a decision to leave the EU. There are two broad potential outcomes following the parliamentary vote, originally scheduled to take place on 11th December, but now postponed pending further “clarification talks” between the UK and the EU leaders:

- The UK leaves the EU with a deal
- The UK leaves the EU with no deal

Brexit

Legislative position

30

- The UK does not plan to make any immediate changes to its own data protection standards, or adoption of the GDPR in connection with its departure from the EU
- The Data Protection Act 2018 (the UK's implementation of the GDPR) will remain in place and the European Union (Withdrawal) Act 2018 will incorporate the GDPR into UK law
- The UK data protection authority is negotiating for “enhanced adequacy” which, if granted, will mean:
 - The EU will consider the UK an equivalent territory in terms of data protection law
 - The UK will be granted a seat on the European Data Protection Board
 - It is not clear if the UK will succeed in negotiating all or part of the enhanced adequacy package and the timing is unclear

Brexit

Data Transfer

31

The legal framework governing the transfer of personal data from the EU to the UK will change after Brexit:

- If a deal is not agreed, post-Brexit the EU will treat the UK as a “third country” and personal data transfers from the EU to the UK will be “restricted” pursuant to Chapter V of the GDPR
- The UK’s preferred negotiating position is to secure an “adequacy” decision, thereby legitimising data transfers from the EU to the UK
- It is not certain that the EC will determine the UK to be adequate, and if it does, when that decision will be made
 - If the UK were deemed adequate this would maintain the free flow of data between the UK and the EU
 - As the outcome is far from certain and timing for the decision is unclear organisations are being advised to adopt safeguards to support the lawful transfer of personal data to the UK in this scenario
 - Be aware of this risk and be ready to consider the adoption of standard contractual clauses (or other appropriate transfer agreements) in the event of a “no-deal” Brexit
 - The flow of data from the UK to the EU will continue unrestricted after Brexit

Brexit

Data Transfers

32

- If a deal is reached, it is anticipated that the status quo on the free flow of data between the UK and the EU will remain unchanged during the transition period
- During the transition period discussions around the adequacy determination will take place and it is hoped that they conclude by the ultimate withdrawal date
- Also consider the ICO's recent guidance on international data transfers which states "*a transfer is only restricted if it is made to a receiver to which the GDPR does not apply*". On that analysis a transfer to a receiver to which GDPR does apply will not be a restricted transfer
- Creation of a "protective bubble" which applies to non-EU located receivers who are nevertheless caught by the extra-territorial reach of Art 3(2) of the GDPR
- This would resolve EU to UK transfers in many instances (as many UK receivers will be compliant with GDPR), but EU organisations outside of the UK may want to look to own regulator guidance for equivalent analysis

CONCLUSION

33

All of this is very complicated ...

**BUT... DO REMEMBER:
WHEN IN DOUBT – ASK YOUR LAWYER!**

**Sapronov & Associates, P.C.
1200 Abernathy Road, Suite 1700
Atlanta, Georgia 30328
Telephone: 770-399-9100
Mobile: 770-309-0462
Facsimile: 770-395-0505
Email: info@wstelecomlaw.com
Website: www.wstelecomlaw.com**

Walt Saprnov



34

770.399.9100
wsaprnov@wstelecomlaw.com



Walt Saprnov has represented corporate clients in telecom transactions, regulation and privacy for over thirty years. He has been named in Georgia Super Lawyers and in the International Who's Who of Telecom Lawyers. Together with his Firm, Saprnov & Associates, P.C., he has negotiated commercial telecom contracts with every major telecom carrier in the U.S. and with many abroad. The Firm also supports clients in privacy compliance before the FCC, the FTC, EU and state regulatory agencies. Mr. Saprnov is a frequent conference speaker and has authored numerous publications on telecommunications law.

For more information, please visit:
www.wstelecomlaw.com

Joseph Srouji



35

Mr. Srouji, based in Paris, France, is Of Counsel to Sapronov & Associates, P.C. and Founding Partner of Srouji Avocats. He is former Senior Counsel for Data Protection & Regulatory Affairs at GE Capital where he worked for over 11 years based in Paris as a specialist in data protection, financial and banking regulation and compliance.

He teaches International Law and Technology Law to graduate students at Université Paris II Panthéon – Assas. He is a member of the Paris Bar and certified CIPP-E.



jsrouji@wstelecomlaw.com

215 rue du Faubourg Saint-Honore

75008 Paris - France

+33 (0) 1 78 64 64 83

Kirk J. Nahra



36

knahra@wileyrein.com

202.719.7335



@KirkJNahrawork



Kirk J. Nahra is a partner with Wiley Rein LLP in Washington, D.C., where he specializes in privacy and information security litigation and counseling, along with a variety of health care and compliance issues. He is chair of the firm's Privacy Practice and co-chair of its Health Care Practice. He assists companies in a wide range of industries in analyzing and implementing the requirements of privacy and security laws across the country and internationally. Mr. Nahra regularly speaks on privacy law issues before a broad variety of audiences, and teaches privacy law at the Washington College of Law at American University.

Kim Roberts



37

Kim Roberts represents global corporates and large employers on their employment law and data privacy strategy in the U.K. and across Europe. She has particular experience with international clients headquartered outside the U.K., specifically those in the U.S. with global operations.

Kim advises on data protection and privacy issues. She specializes in advising cross border European clients on their data privacy obligations, data privacy policies and employee data management. Kim advises clients on developing law and practice in the EU including the GDPR and on obligations when transferring data between the EU and the U.S., including advice on Model Clauses and the Privacy Shield.

Kim speaks regularly at client events and seminars and commentates in the U.K. national press on employment law and data privacy matters and developments.



**44 (0) 20 7551 2133
kroberts@kslaw.com**

3. Part III – The Age of Turmoil (April, 2020)

SAPRONOV & ASSOCIATES, P.C.

ATTORNEYS AT LAW

info@wstelecomlaw.com

www.wstelecomlaw.com

1300 I STREET, NW, SUITE 400
WASHINGTON, D.C. 20005
TEL. 770.309.0462

5555 GLENRIDGE CONNECTOR
SUITE 200
ATLANTA, GEORGIA 30342
TEL. 770.399.9100

10 VOZDVIZHENKA STREET
MOSCOW, RUSSIA 125009
+7 985 920-89-93

A SPECIAL CLIENT ALERT¹

Privacy in the New World Order

Part III: The Age of Turmoil

April 21, 2020

Continuing our collaboration with Thomson Reuters, we are pleased to announce Part III of our “*Privacy in the New World Order*,”² series: “*The Age of Turmoil*.” This program³ discusses privacy developments, both in the U.S. and abroad, following world wide disruptions to global trade, health, and investment. These developments will affect every attorney involved with U.S., U.K., and European Union (“EU”) privacy protections, whether in compliance or in transactional matters. The discussion is about privacy laws, here and abroad, and how they function (or should) in the wake of rapidly unfolding, uncharted global disruptions: “Brexit” (British exit from the EU), newly expanded U.S. regulations under the Committee for Foreign Investment in the U.S. (“CFIUS”), and – most importantly - the privacy implications of exchanging health related information in response to COVID-19 (“Corona virus”).

Here is a brief synopsis of the program.

¹ THIS SPECIAL CLIENT ALERT IS PROVIDED COMPLIMENTARY TO CLIENTS AND FRIENDS OF SAPRONOV & ASSOCIATES, P.C. FOR TUTORIAL PURPOSES ONLY AND IS NOT TO BE CONSTRUED AS A LEGAL OPINION OR LEGAL ADVICE. PLEASE CONTACT US AT (770) 399-9100, OR AT INFO@WSTELECOMLAW.COM IF YOU HAVE SPECIFIC QUESTIONS ABOUT THIS ALERT – OR IF YOU WISH TO BE REMOVED FROM OUR MAILING LIST.

² Parts I (“Compliance”) and II (“Globalization”) of this series are available upon request at info@wstelecomlaw.com.

³ http://westlegaledcenter.com/program_guide/course_detail.jsf?videoCourseId=100278512&ADMIN_PREVIEW=true.

I. Privacy and the Pandemic

As the Corona virus envelops the world and authorities scramble to contain it, privacy is the least of its victims' worries. The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and other privacy laws surely were not enacted to create life-threatening treatment compliance delays. Viewed in that context, Corona virus privacy protection would seem oxymoronic.

Or maybe not. Even as governments muster resources to identify Corona's reach with the help of Google and the like, location data and other private health information amassed by the Internet giants will remain in their possession long after the virus is gone. A few alarms have already been raised, especially about "Big Tech" control over Corona related personal data.⁴ Sen. Edward Markey (D. MA), a long-time telecom policy veteran, has expressed concern in writing to the Office of Science and Technology Policy over the use of geolocation data by U.S. government "partnerships" (an Orwellian thought) with Google and the like. Consent to use this information (as required for hospital patients by HIPAA) or the right to demand one forgets it (as required by the GDPR) is probably not a foremost concern of such patients while the virus spreads; someday soon it might be.

This session will focus on a series of important issues about the virus and the health care system that are arising as we speak. These issues will be discussed, including a series of new developments related to the U.S. government's activities to enforce the HIPAA rules, as well as some of the international implications in this area.

II. Privacy Developments Around the Globe

A. General Data Protection Regulation ("GDPR") and the EU

The GDPR is nearly at the two-year mark and the sentiment among EU regulators is that (with its grace period now expired) it is ripe for more stringent enforcement action. While many companies have made significant strides in GDPR compliance, hiring necessary resources and reinforcing internal privacy governance, there remain plenty of outliers, including among big tech. We take a look at some enforcement priorities for EU regulators, review a sampling of enforcement actions (indicative of things to come) and spend time on EU class actions for privacy violations – still stuck at the starting block. Finally, we conclude with a look at a few trends and difficulties that companies face as they strive for GDPR compliance. Is the GDPR already outdated?

B. Privacy in the U.K. after Brexit

The U.K. left the EU on January 31, 2020 and is now engaged in a complex negotiation of its future trading relationship with the EU for a transition period, which will last until the end of 2020. This session will focus on how Brexit affects the U.K.'s privacy laws, the application

⁴ See <https://www.politico.com/news/2020/03/18/big-tech-coronavirus-134523>.

of the GDPR in the U.K., and how to manage data flows between the EU and the U.K., and the U.K. and the rest of the world.

III. Privacy and Foreign Investment in the U.S.

Global turmoil is not limited to Corona. Geo-political tensions are as high as ever – especially between the U.S. and China (accused by some of creating the virus). As a consequence of that fraught relationship, the U.S. has expanded its CFIUS regulations, commonly known as the Foreign Investment Risk Review Modernization Act of 2018, or “FIRMA,”⁵ and the government’s most stringent tool for scrutinizing foreign investments, most recently to those that touch on privacy. While not specifically aimed at China, the new regulations focus on investments in a wide range of businesses from health care to hotels to banks - almost any enterprise that gathers, uses or maintains the “sensitive” personal health or financial information of US citizens.

Our in-depth discussion can be found at http://westlegaledcenter.com/program_guide/course_detail.jsf?videoCourseId=100278512&ADMIN_PREVIEW=true. Our panel includes: Kirk Nahra of Wilmer Hale, discussing privacy implications in the face of Covid-19; Joseph Srouji, Of Counsel to Saprnov & Associates, P.C., discussing the GDPR; Kim Roberts of King & Spalding, discussing Brexit and the impact on EU data privacy laws in the UK; James Wholey of Phillips Lytle, discussing U.S. restrictions on foreign investment. Walt Saprnov will serve as moderator. We hope to see you there. Be SAFE during these difficult times – and MAY GOD BLESS US ALL.

⁵ For a detailed presentation on CFIUS and FIRMA expansion, see our webinar for Thomson Reuters, “Negotiable Hostilities: Doing Telecom Deals with Russia in the Sanctions Era,” (available at https://westlegaledcenter.com/program_guide/course_detail.jsf?videoCourseId=100267557&ADMIN_PREVIEW=true).

Privacy in the New World Order

CONTINUING LEGAL EDUCATION THOMSON REUTERS

March 31, 2020

**Moderated by Walt Saprnov
Saprnov & Associates, P.C.
5555 Glenridge Connector, Suite 200
Atlanta, Georgia 30342
www.wstelecomlaw.com
(770) 399-9100**

Privacy in the New World Order

Part III: The Age of Turmoil

2

- Introduction - Recent Global Privacy Developments
- Brexit & the GDPR
- New CFIUS Regulations
- Emerging Privacy Concerns
 - Cross-border privacy protection
 - U.S. foreign investment restrictions
 - Stopping Covid-19 (the Corona Virus)
 - Balancing privacy and healthcare

INTRODUCTION

Recent Privacy Developments

- General Data Protection Regulation (“GDPR”)
 - Increasing international acceptance
 - Including potential U.S. state GDPR-like legislation
 - So far California - who will be next?
 - Possible U.S. federal legislation
- Brexit (U.K. left the European Union January 31, 2020)
 - Privacy implications for U.K.-EU cross-border info exchange
- U.S. restrictions on foreign investment
 - The Committee on Foreign Investment in the U.S. (“CFIUS”)
 - New regulations: Foreign Investment Risk Review Modernization Act of 2018 (“FIRRMA”)

INTRODUCTION (*Cont.*)

4

- New Foreign Investment restrictions
 - Expanded reach – including commercial transactions
 - Advance notice requirements: burden on parties
 - Draconian penalties for non-compliance (up to deal value)
 - Now broadly include any foreign investment that includes access to personal data / private information

INTRODUCTION (*Cont.*)

- But most important is the Covid-19 Pandemic
 - Travel restrictions / quarantines / other governmental protections
 - Requires access to personal medical information and raises numerous privacy concerns
 - Health data is always sensitive
 - Largely protected under U.S. and foreign laws, including GDPR, U.S. HIPAA and State privacy laws
 - Escalating daily virus containment efforts
 - How to balance privacy with health care concerns?

Privacy and the Corona Virus

6

Kirk J. Nahra
Wilmer Cutler Pickering Hale
and Dorr LLP
1875 Pennsylvania Avenue, NW
Washington, DC 20006
kirk.nahra@wilmerhale.com
(202) 663-6128

Privacy and the Corona Virus

7

- A variety of key privacy concerns, for health care providers, public officials and employers
- Complexity of competing laws and policy goals
- Different rules in different countries
- Lots of confusion and mis-information
- But emerging best practices and critical goals

HIPAA

8

- Health Insurance Portability and Accountability Act
- Reminder - Is not an overall medical privacy law – protects certain information when it is held by certain kinds of entities in certain situations
- Compare with GDPR – where health information is protected regardless of who has it

HIPAA – Health Care Providers

9

- Major impact of HIPAA in this situation is for health care providers
- HIPAA rules envision these kinds of scenarios – permit disclosures by health care providers for public health purposes, where required by law, and where appropriate for treatment, payment and health care operations
- Rules envision reasonable covered entity judgment – and anticipated a broad variety of scenarios
- We are also seeing a variety of new tensions between the HIPAA rules and other goals or commercial developments

The HIPAA Rules and Health Care

10

- Issues related to patient access to their own information - balancing privacy/security concerns with need for access
- Broad range of “non-HIPAA” health data situations – and how unregulated entities (*e.g.*, tech companies) may be able to help the system but aren’t inside the HIPAA system
- Social determinants of health

HIPAA - Health Care Providers

11

- New guidance from administration
- Permitted use of telehealth – waiver of security rule provisions
- Allows convenience of telehealth without need to be concerned about specific security rule compliance
- General goal of making treatment consultations easier for doctors and patients
- All good – promotes confidence and comfort
- Please still try to be smart (don't do the telehealth visit while you are at Starbucks)

HIPAA – Health Care Providers

12

- ❑ Additional Waivers - privacy notices, sharing with friends and family, requests for restrictions and confidential communications
- ❑ Not as clear what the point of these are
- ❑ Not areas where there has been traditional enforcement
- ❑ Issue with restrictions and confidential communications – we have seen an increase in domestic violence already, this may run counter
- ❑ So flexibility, no concern about enforcement, still be smart

HIPAA - Employers

13

- For most employers, HIPAA is only relevant for the employee health benefits plan
- Relates to information about health insurance claims sent through the benefits process
- Most employers don't get this information in identifiable form, and there is a substantial time lag in any event
- Other health information held by employers – from workers comp, disability, FMLA, doctors notes, office gossip – is not subject to HIPAA
- Doesn't mean there aren't rules (*e.g.*, ADA), but HIPAA generally isn't one of them

ADA

14

- ADA (Americans with Disabilities Act) – not just a law dealing with disabilities
- Law dictates employer practices in relation to confidential medical information
- Creates strict limits on the disclosure of personally identifiable health information
- Requires careful thought from employers
- Seldom a reason to disclose a name – but no real obligation to make sure that no one can identify the person
- Be reasonable and thoughtful – recognize the competing interests

Data Security Concerns Because of Remote Work

15

- Remote work – particularly if not typical – creates meaningful security risks
- Scammers/hackers/malicious actors are in active mode
- Employees need to be trained and given guidance on what remote work means for security
- Careful attention to access controls
- Importance of incident response planning
- Importance of back-up systems and contingency planning
- Test while you can

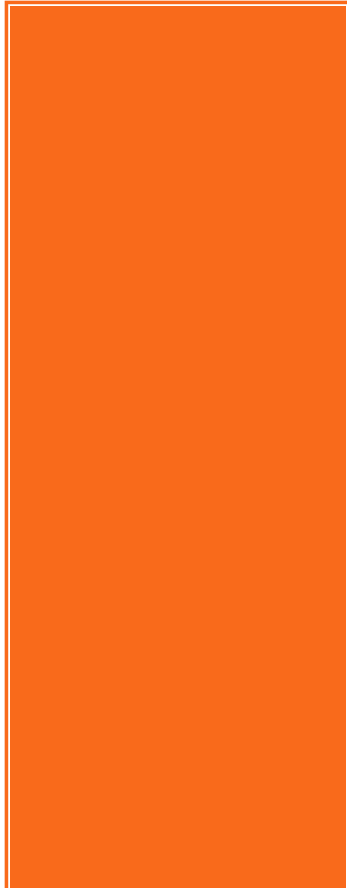
Other Issues

16

- Unless you are a health care provider, seldom an obligation to report information
- Many health departments don't want the reports at this time – they are focusing on reports from health care providers
- Be thoughtful and smart – protecting health and safety of employees and customers is critically important
- Privacy laws typically can bend in these situations – but not an excuse to give up on privacy
- Be thoughtful and responsible, and err on the side of not disclosing names unless really necessary

General Data Protection Regulation (“GDPR”)

17



Joseph Srouji

Of Counsel

Sapronov & Associates, P.C.

215 rue du Faubourg Saint-Honore

75008 Paris – France

jsrouji@wstelecomlaw.com

+33 (0) 1 78 64 64 83

GDPR Principles

18

- Reminder: main principles
 - Extraterritoriality: GDPR applies when controller/processor processes personal data on EU territory; or when controller/processes is not established in the EU but processes personal data relating to data subjects in the EU
 - Accountability: data controller must implement internal mechanisms and procedures to demonstrate compliance with data protection rules
 - Reinforcement of data subject's rights:
 - Transparency: controller must provide information about the data processing
 - Consent: stricter requirements
 - New rights: right to data portability
 - Reinforced rights: right of access and right to object
 - Increased sanctioning power

EU Enforcement Priorities for 2020

19

- French regulator CNIL highlights its enforcement priorities for 2020:
 - Safeguarding health data
 - Use of geolocation data
 - Use of cookies and other web tracking technology
- Prior year focused on data subject rights, rights of minors and responsibilities of controllers and processors

Examples of Enforcement

20

- Examples of sanctions at the 2-year mark
 - Unsolicited promotional calls without consent or without taking into account the opposition of data subjects
 - Failure to obtain consent for the processing of data for marketing purposes
 - Incorrect and non-transparent information on data processing provided to data subjects
 - Failure to implement sufficient technical and organizational measures
 - Retaining irrelevant data such as insulting comments or comments related to data subject's health

Class Actions in the EU (1/3)

21

- Article 80 GDPR: data subjects' right to mandate a non-profit organization or association, which will:
 - Lodge a complaint on their behalf with a supervisory authority (Article 77 GDPR);
 - Exercise on their behalf the right to an effective judicial remedy against the supervisory authority or the controller or the processor (Articles 78 and 79 GDPR);
 - Exercise on their behalf the right to obtain compensation, in the event of material or non-material damage (Article 82 GDPR).

- Article 37 *Loi informatique et libertés*: the class action may aim to put an end to any breach of this law or the GDPR, and/or may aim to hold the company/person who caused the damage liable in order to obtain compensation for material and moral damages suffered.

Class Actions in the EU (2/3)

22

- Recent cases
 - On May 25, 2018, the association NONE OF YOUR BUSINESS (NOYB) filed a complaint with the CNIL against Google, claiming that the company does not sufficiently inform users of android smartphones of the future use of their data
 - On May 25, 2018, the French association LA QUADRATURE DU NET filed five claims against the GAFA and LinkedIn with the CNIL on behalf of 12,000 people. They consider that these companies do not comply with GDPR in the way they collect the consent of Internet user
 - In November 2018 the NGO Internet Society France sent a formal notice to Facebook to respond to seven main grievances. According to the association, each Internet user could be compensated up to 100 million euros if it brings together 100 000 people on the procedure

Class Actions in the EU (3/3)

23

- Result of these class actions:
 - The CNIL imposed on January 21, 2019, a meager fine of 50,000 euros against Google, which has appealed
 - NOYB and LA QUADRATURE DU NET complaints did not include claims for damages (CNIL was not able to take a position)
 - Facebook did not respond so the NGO filed a lawsuit against the company in the French courts in September 2019, in particular so that the plaintiffs could be compensated for these breaches. The case is still pending in the courts

Data Transfers Outside de EU (1/2)

24

- Data Protection Commissioner (DPC) vs Facebook Ireland Limited and M. Schrems (C-311/18)
 - Case brought before the DPC by Austrian lawyer Max Schrems who wanted to stop personal data flows between Facebook's headquarters in Ireland and its parent company in California:
 - The European Court of Justice must decide whether Facebook is properly protecting those data transfers
 - Facebook claims that data transfers in the USA are sufficiently regulated by standard contractual clauses (“SCC”)
 - The DPC holds that SCC are no longer sufficient given the widespread surveillance activities carried out by the US

Data Transfers Outside de EU (2/2)

25

- The Advocate General delivered his Opinion on 19 December 2019:
 - The principles of SCC are valid
 - They are incompatibilities between European law and massive and indiscriminate US intelligence monitoring programs
 - Supervisory authorities and controllers must assume their responsibilities and apply, where necessary, the obligation to suspend or prohibit transfers where countries do not provide sufficient guarantees

Coronavirus and Health Data

26

- Divergent recommendations from European supervisory authorities concerning the collection and processing of employee health data to prevent the spread of the coronavirus.

- French supervisory authority - CNIL. Companies have to:
 - Implement appropriate measures : travel restrictions limiting meetings, reminding basic hygiene requirements...
 - Implement preventive measures : trainings, having appropriate organization and resources
 - Not adopt measures that could infringe on employee's private life, including collection of health data
 - Refrain from collecting in a general and systematic manner information to determine medical symptoms of employees
 - If a person is suspected of having contracted the virus, the company may collect date and identity and implement measures for quarantine, distance working...

Privacy Regulatory Trends

27

- Increasingly aggressive regulators (2 year grace period reached)
- Data subject requests: more sophisticated and used as a lever point in pre-litigation or during litigation
- EU standards increasingly the norm (*i.e.*, US state laws increasingly poised to follow CA model)
- IT security continues to be key differentiator for privacy compliance: regulators expect high standards for data protection (continually evolving as technology advances)
- ePrivacy Regulation on the horizon (still)
- Some countries like Turkey and India are implementing standards based on EU model but with additional complexity

Challenges with GDPR Compliance

28

- Some difficulties with GDPR compliance since implementation:
 - Difficulties in identifying controller/processor roles;
 - Conflict of law between the implementation of procedures related to whistleblowers and data protection;
 - Conflicts between the “public interest” in the context of epidemics (coronavirus) and the necessary protection of privacy and health data protection;
 - ...

WHAT BREXIT MEANS FOR U.K. DATA PROTECTION

29



Kim Roberts
King & Spalding
125 Old Broad Street
London, United Kingdom
EC2N 1AR
kroberts@kslaw.com
+44 20 7551 2133

THE TRANSITION PERIOD

30

- The U.K. left the European Union on 31 January 2020
- The period until the end of 2020 is a transition period during which the U.K. and the EU will negotiate trade deals
- During the Transition Period the status quo will remain
 - GDPR and national law remains unchanged in the U.K.
 - Data transfers can continue to be managed under the existing framework



2021 AND BEYOND

31

- GDPR will not apply after the Transition Period
- The U.K. has implemented national law (The Data Protection Act 2018 “DPA”) which mirrors GDPR
- The provisions of GDPR will be incorporated directly into U.K. law from the end of the transition period, and will sit alongside the DPA



2021 AND BEYOND

32

- In practice there will be no change to the application of core principles of existing data protection law to the U.K. after the Transition Period
- However, much depends on the nature of the deal negotiated between the U.K. and the EU, in particular how the position on data transfers from the EEA to the U.K. will be resolved



REPRESENTATIVES

33

- Businesses based in the U.K. which have no branch, office or other establishment in any other EU or EEA state, but which either:
 - offer goods or services to individuals in the EEA;
or
 - monitor the behaviour of individuals in the EEA,
- are required to appoint a representative in the EEA in compliance with GDPR after Brexit



U.K. AS SUPERVISORY AUTHORITY

34

- After Brexit the ICO will remain the independent supervisory authority regarding the U.K.'s data protection legislation
- During the transition period the ICO will engage in the co-operation and consistency mechanism under GDPR and continue to be a lead supervisory authority
- The U.K. government plans to maintain close working relationships between the ICO and the EU supervisory authorities after Brexit



U.K. AS SUPERVISORY AUTHORITY

35

- Can a business which carries out cross-border processing after Brexit continue to recognise the ICO as lead supervisory authority?
 - Review EDPB guidance, and consider which other EU and EEA supervisory authority will become lead authority on exit date
 - Businesses with multiple establishments or which target customers in a number of EU jurisdictions may need to recognise more than one supervisory authority



DATA TRANSFERS FROM THE U.K.

36

- Restricted transfers from the U.K. to countries outside the U.K., including to the EEA, will be subject to transfer rules under the U.K. regime, which will mirror the current GDPR rules
- U.K. government has confirmed that regular transfers from the U.K. to the EEA will not be restricted after Brexit
- There will be transitional provisions for a U.K. adequacy decision to cover these transfers



U.K. TO RECOGNISE “ADEQUACY”

37

- Rules on transfers to countries outside the EEA will remain similar to current GDPR rules
- Although the U.K. will make its own adequacy decisions after exit, the U.K. government has confirmed that it intends to recognise existing EU adequacy decisions, approved EU SCCs and BCRs wherever possible.



TRANSFERS OF DATA FROM EEA TO U.K.

38

- Rules on transfers from EEA to countries outside the EEA (including the U.K.) will remain similar to current GDPR rules
- Reliance on existing transfer mechanisms to legitimise data transfers
 - Standard Contractual Clauses
 - Approved Binding Corporate Rules
 - U.K./US Privacy Shield (in development)



U.S. Restrictions on Foreign Investment CFIUS

39

James K. Wholey
Phillips Lytle, LLP
1101 Pennsylvania Avenue NW
Suite 300
Washington, DC 20004-2514
jwholey@phillipslytle.com
(202) 617-2714



U.S. Restrictions on Foreign Investment

CFIUS

40

- FIRRMA (Foreign Investment Risk Review Modernization Act of 2018)
 - Greatly expanded CFIUS regulations
 - Expanded jurisdiction over direct foreign investment into U.S.
 - Recently published by Department of Treasury (31 C.F.R. §800-802)
 - Focused on even more *non-controlling investments*
 - So-called TDI (Technology, **Data** & Infrastructure) industries
 - **Data** portion is what's new

U.S. Restrictions on Foreign Investment

CFIUS

41

- Specifically, regulations point to foreign investment in businesses that:
 - Collect, Maintain (or plan to) or Utilize “Sensitive personal data of U.S. Citizens”

- **“Sensitive Personal Data of US Citizens”**
 - Under the regs, the above term applies to any business:
 - that directly or indirectly collects or maintains genetic test results of U.S. citizens
 - US businesses that collect or maintain a high volume of records
 - 11 specified categories of sensitive personal data
 - including geolocation data; physical or mental health information; biometric data; insurance application data; detailed financial data; government security clearance information; and nonpublic electronic data between business users of the target’s products

U.S. Restrictions on Foreign Investment

CFIUS

42

- Reminder:
 - The investments specified in the regulations are NOT prohibited
 - but such investments, if of the above described nature, trigger a filing requirement
 - Such filing, if required or advisable, should be factored into the time, cost and risk elements of the contemplated investment
 - CFIUS review is not triggered if the investment does NOT:
 - confer membership, nomination or observer rights on the board of the target entity
 - involvement, other than voting of shares, in substantive decision making
 - access to material nonpublic information in possessed by the target or its US subsidiary

U.S. Restrictions on Foreign Investment

CFIUS

43

- Data specified in the regs:
 - Financial data that could be used to analyze financial distress or hardship
 - Consumer report data (with some exceptions)
 - The data sets in applications for health, long term care, professional liability, mortgage or life insurance
 - Data relating to individual health condition
 - Non-public messaging or email between a business's users
 - Geolocation data, whether from cell, GPS, Wi-Fi points or wearable device
 - Biometric enrollment data (face, retina, fingerprint, voice)
 - Data stored for purpose of generating or renewing Federal government ID
 - Data re: U.S. Federal security clearances
 - Data in application for such clearance
 - Results of an individual's genetic tests

U.S. Restrictions on Foreign Investment

CFIUS

44

- Exclusions:
 - Court records and other matters already in the public record
 - Data maintained by US employers regarding its own employees

- Obvious implications for potential investments in:
 - health care companies
 - insurance companies;
 - information web “apps”
 - TELECOMMUNICATIONS services carriers and their vendors
 - Cloud companies
 - US government contractors
 - any foreign company that has US operations
 - Who knows what else?!

CONCLUSION

45

All of this is very complicated ...

**BUT... DO REMEMBER:
WHEN IN DOUBT – ASK YOUR LAWYER!**

**Sapronov & Associates, P.C.
5555Glenridge Connector, Suite 200
Atlanta, Georgia 30342
Telephone: 770-399-9100
Mobile: 770-309-0462
Facsimile: 770-395-0505
Email: info@wstelecomlaw.com
Website: www.wstelecomlaw.com**

Walt Saprnov



46

770.399.9100
wsaprnov@wstelecomlaw.com



Walt Saprnov has represented corporate clients in telecom transactions, regulation and privacy for over thirty years. He has been named in Georgia Super Lawyers and in the International Who's Who of Telecom Lawyers. Together with his Firm, Saprnov & Associates, P.C., he has negotiated commercial telecom contracts with every major telecom carrier in the U.S. and with many abroad. The Firm also supports clients in privacy compliance before the FCC, the FTC, EU and state regulatory agencies. Mr. Saprnov is a frequent conference speaker and has authored numerous publications on telecommunications law.

For more information, please visit:
www.wstelecomlaw.com

kirk.nahra@wilmerhale.com

202.663.6128



@KirkJNahrawork



Kirk J. Nahra is a partner with Wilmer Cutler Pickering Hale and Dorr LLP in Washington, D.C., where he specializes in privacy and information security litigation and counseling, along with a variety of health care and compliance issues. He is co-chair of the firm's Privacy and Cybersecurity Practice. He assists companies in a wide range of industries in analyzing and implementing the requirements of privacy and security laws across the country and internationally. Mr. Nahra regularly speaks on privacy law issues before a broad variety of audiences, and teaches privacy law at the Washington College of Law at American University.

Joseph Srouji



48

Mr. Srouji, based in Paris, France, is Of Counsel to Sapronov & Associates, P.C. and Founding Partner of Srouji Avocats. He is former Senior Counsel for Data Protection & Regulatory Affairs at GE Capital where he worked for over 11 years based in Paris as a specialist in data protection, financial and banking regulation and compliance.

He teaches International Law and Technology Law to graduate students at Université Paris II Panthéon – Assas. He is a member of the Paris Bar and certified CIPP-E.



jsrouji@wstelecomlaw.com

215 rue du Faubourg Saint-Honore

75008 Paris - France

+33 (0) 1 78 64 64 83

Kim Roberts



49

Kim Roberts represents global corporates and large employers on their employment law and data privacy strategy in the U.K. and across Europe. She has particular experience with international clients headquartered outside the U.K., specifically those in the U.S. with global operations.

Kim advises on data protection and privacy issues. She specializes in advising cross border European clients on their data privacy obligations, data privacy policies and employee data management. Kim advises clients on developing law and practice in the EU including the GDPR, and on obligations when transferring data between the EU and the U.S., including advice on Model Clauses and the EU/U.S. Privacy Shield.

Kim speaks regularly at client events and seminars and commentates in the U.K. national press on employment law and data privacy matters and developments.



**44 (0) 20 7551 2133
kroberts@kslaw.com**

jwholey@phillipslytle.com
202.617.2714



Mr. Wholey has broad experience at the intersection of federal government, national security and international business. His specific focus is on the legislative, policy and compliance issues involved in international investment, trade and business development. Through his international business and federal government relations practice, he assists clients with transnational compliance matters (Foreign Corrupt Practices Act, EAR, ITAR, export licensing and involvement with various sanctions regimes) and works frequently with the Administration and Capitol Hill. He spent more than a decade as a senior staff member for several U.S. senators, including three years as chief of staff to then-Senate Leader Bob Dole (R-KS), for whom he also handled trade and telecommunications issues.

4. Part IV – The Privacy Shield Falls (December, 2020)

SAPRONOV & ASSOCIATES, P.C.

ATTORNEYS AT LAW

info@wstelecomlaw.com

www.wstelecomlaw.com

1300 I STREET, NW, SUITE 400
WASHINGTON, D.C. 20005
TEL. 770.309.0462

5555 GLENRIDGE CONNECTOR
SUITE 200
ATLANTA, GEORGIA 30342
TEL. 770.399.9100

10 VOZDVIZHENKA STREET
MOSCOW, RUSSIA 125009
+7 985 920-89-93

A SPECIAL CLIENT ALERT¹

Privacy in the New World Order

More Turmoil: the Privacy Shield Falls

December 4, 2020

Continuing our collaboration with Thomson Reuters, we are pleased to announce that Part IV of our “*Privacy in the New World Order*,”² series is now available for purchase.³ This latest webinar – aptly titled “*More Turmoil: the Privacy Shield Falls*” - addresses just that: the continued turmoil surrounding international privacy rules (and how to comply with them) for companies, especially those in the U.S. and the U.K., that engage in data transfer with EU jurisdictions. In today’s global economy, this sweeps in just about everyone doing business abroad.

Moderated by Walt Sapronov and Joseph Srouji of our Firm, the program discusses the implications of the July 16, 2020 decision of the EU High Court of Justice of the European Union in *Schrems*, and *Facebook Ireland v. Data Protection Commissioner* (“*Schrems II*”). The EU Court of Justice found the safe harbor for U.S. compliance with EU privacy law, the so-called “Privacy Shield,” to be invalid. The Privacy Shield was a framework designed by the U.S. Commerce Department and the EU Commission for complying with data protection requirements for the cross-border transmission of personal data, largely governed by the EU General Data Protection Regulation (“GDPR”). Adding to the uncertainty now surrounding cross-border data flows is the looming impact of BREXIT and the U.S. elections. The panel of experts will discuss how to deal with

¹ THIS SPECIAL CLIENT ALERT IS PROVIDED COMPLIMENTARY TO CLIENTS AND FRIENDS OF SAPRONOV & ASSOCIATES, P.C. FOR TUTORIAL PURPOSES ONLY AND IS NOT TO BE CONSTRUED AS A LEGAL OPINION OR LEGAL ADVICE. PLEASE CONTACT US AT (770) 399-9100, OR AT INFO@WSTELECOMLAW.COM IF YOU HAVE SPECIFIC QUESTIONS ABOUT THIS ALERT – OR IF YOU WISH TO BE REMOVED FROM OUR MAILING LIST.

² Parts I (“Compliance”), II (“Globalization”) and III (“The Age of Turmoil”) of this series are available upon request at info@wstelecomlaw.com.

³ http://westlegaledcenter.com/program_guide/course_detail.jsf?videoCourseId=100291865&ADMIN_PREVIEW=true.

compliance and other data security concerns in this age of turmoil. These include Kenneth N. Rashbaum of Barton, LLP, Kim Roberts of King & Spalding, and Nicholas Oldham, Global Chief Privacy and Data Governance Officer at Equifax.

Here is a brief synopsis of the program.

I. Schrems II Decision (C-311/18)

We kick off the program with an overview by Joseph Srouji of the of the *Schrems* decisions, beginning with the original 2013 Complaint to the Irish Data Protection Commission, and concluding with the European Union Court of Justice’s decision, which ended the Privacy Shield. Joseph highlights the arguments on each side, discusses the Court’s ruling and concludes with how the decision will impact consumers and the treatment of privacy information going forward.

II. The US Data Protection Mosaic

Next, Ken N. Rashbaum discusses U.S. privacy compliance following the strike down of the Privacy Shield. Ken discusses how even without the safe harbor of the Privacy Shield, compliance with state privacy law and so-called “Standard Contract Clauses” can mitigate the consequences of GDPR violations.

III. WHAT BREXIT MEANS FOR U.K. DATA PROTECTION

We welcome back Kim Roberts, who continues to keep us updated on the implications of Brexit and the GDPR in light of the United Kingdom’s departure from the European Union. She educates us on what to expect after the Transition Period (end of 2020), discusses the U.K.’s new national law and how this all realistically fits into day-to-day privacy practice. This session will focus on how Brexit affects the U.K.’s privacy laws, the application of the GDPR in the U.K., and how to manage data flows between the EU and the U.K., and the U.K. and the rest of the world.

IV. INSIGHTS FOR BUILDING A GLOBAL PRIVACY PROGRAM FROM A CHIEF PRIVACY OFFICER

Our final speaker brings us practice pointers from the view of a Chief Privacy Officer. Nick Oldham, Global Chief Privacy and Data Governance Officer at Equifax, discusses how to merge the various privacy requirements and practically implement them into practice. Nick outlines the practical steps for implementing an in-house Global Privacy Program that encompasses legal as well as cultural and organizational concepts.

We conclude the program with a round table discussion of what might (or might not) change as a result of the recent U.S. elections. Again, this in-depth discussion can be found at http://westlegaledcenter.com/program_guide/course_detail.jsf?videoCourseId=100291865&ADMIN_PREVIEW=true. For a copy of any of our previous pod-casts in this series, please contact us at info@wstecomlaw.com.

We take this opportunity to wish you and yours Merry Christmas, Happy Holidays, and (especially in these difficult times) a SAFE and prosperous New Year.

Privacy in the New World Order

CONTINUING LEGAL EDUCATION THOMSON REUTERS

November 12, 2020

**Moderated by Walt Saprnov
Saprnov & Associates, P.C.
5555 Glenridge Connector, Suite 200
Atlanta, Georgia 30342
www.wstelecomlaw.com
(770) 399-9100**

Privacy in the New World Order

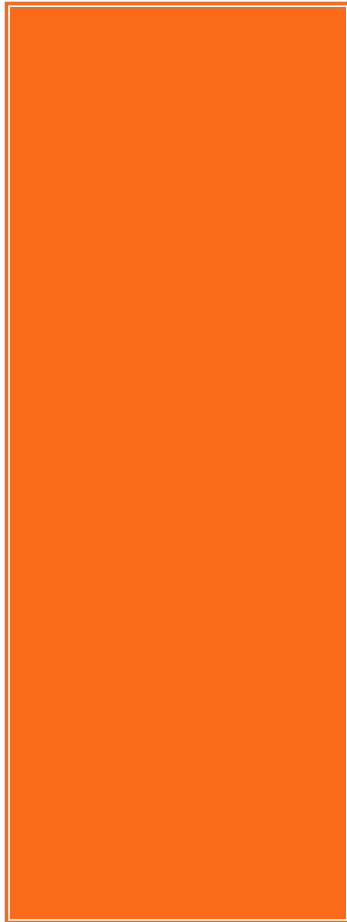
Part IV: More Turmoil – the Privacy Shield Falls

2

- Introduction - Compliance with GDPR after Schrems II
- Privacy Shield Struck Down
 - Overview
 - Implications / Compliance for the EU
 - Implications / Compliance for the U.S.
 - Updates / Changes to Brexit
 - View from a Chief Privacy Officer – Practice Pointers

Schrems II Decision (C-311/18)

3



Joseph Srouji
Of Counsel
Sapronov & Associates, P.C.
222 Boulevard Saint Germain
75007 Paris – France
jsrouji@wstelecomlaw.com
+33 (0) 1 78 64 64 83

Schrems II Decision (C-311/18)

4

- Background: the *first* Schrems' decision
 - June 25, 2013: First complaint of Maximillian Schrems to the Irish Data Protection Commission (DPC):
 - Request to prohibit Facebook from transferring personal data to US
 - Legal argument: insufficient protections against the surveillance activities carried out by US public authorities
 - Complaint dismissed by the DPC relying on Commission Decision 2000/520 Safe Harbor
 - Mr. Schrems appealed to the Irish High Court
 - Irish High Court referred for a preliminary ruling to the European Union Court of Justice (EUCJ)
 - On October 6, 2015 EUCJ invalidated the Commission's Safe Harbor Decision

Schrems II Decision (C-311/18)

5

- Background: steps towards the second Schrems' decision
 - Referring court annulled the rejection of the complaint and referred back to DPC
 - Schrems reformulated his complaint as Facebook stated that large part of transfers took place on the basis on Standard Contractual Clauses (SCC):
 - Facebook make personal data transferred available to US authorities
 - The use of those data is incompatible with article 7, 8 and 47 of the European Charter of Human Rights – no legal remedy available
 - SCC cannot justify such a transfer
 - Asks DPC to prohibit Commission Decision 2010/87 on SCC
 - On May 31, 2016 the DPC referred the matter to the High Court to question ECJ on validity of Commission Decision 2010/87

Schrems II Decision (C-311/18)

6

- Advocate General's Opinion (December 19, 2019)
 - There are no factors of such a nature that could affect the validity of Commission Decision 2010/87:
 - SCC are not binding on third country authorities – but this is not sufficient to invalidate the Decision
 - Conformity of this Decision will depend on whether there are robust mechanisms in place to ensure that a transfer can be suspended or cancelled
 - Such mechanism exists : data controllers and supervisory authorities have the obligation, in certain cases, to suspend or cancelled the transfer
 - Questions the validity of Commission Decision 2016/1250 on Privacy Shield

Schrems II Decision (C-311/18)

7

- EUCJ's decision on July 16, 2020 (Schrems II)
 - Invalidates Commission Decision 2016/1250 – cancelling Privacy Shield:
 - Disclosure of personal data to a third party, such as public authority constitutes an interference with fundamental rights
 - No requirements equivalent to that guarantee by article 52 of the Charter
 - No legal remedies possible for data subjects in European Union whose personal data are transferred in the US
 - No level of protection equivalent to article 47 of the Charter
 - Validates the Commission Decision 2010/87 (followed Advocate General's opinion):
 - The validity of SCC depended on effective mechanisms to ensure that level of protection required by EU is respected and that transfer can be suspended or cancelled
 - EUCJ found that such mechanisms exist

Schrems II Decision (C-311/18)

➤ Impact of Schrems II

- Data exporter and data importer are expected to perform a data transfer adequacy assessment that should take into account:
 - Contractual stipulations between exporter and importer
 - Relevant elements of the legal system of the third country concerning possible access by public authorities of third country to transferred data
 - Assess the adequacy of the level of protection offered by the third country as detailed in article 45 § 2 of the GDPR
- No grace period : Privacy Shield is invalidated and transfers that occur on the basis of Privacy Shield are now illegal
- Binding Corporate Rules fall in same bucket as SCC

The US Data Protection Mosaic

9

Kenneth N. Rashbaum
Partner

Barton, LLP

711 Third Avenue

14th Floor

New York, NY 10017

212.885.8836

krashbaum@bartonesq.com

BARTON
Discover Better Law

Privacy in the New World Order

Part IV: The US Mosaic

10

- Introduction - Recent Global Privacy Developments
- Privacy Shield Struck Down: Now What?
 - Overview
 - Over 4,000 US companies had been registered with the Framework
 - How do they proceed to meet new cross-border data protection schemes and the laws of 54 domestic jurisdictions?

Standard Contract Clauses

- Survived the challenge in *Schrems II*, barely
- Authorities in Ireland and Germany have questioned their continued validity
- Uncertainty abounds and that slows down business transactions
 - Many agreements are drafted by non-lawyers who often confuse and muddy compliance representations

Help on the Way

- Data Protection action in the US is primarily at the state level
- State laws in effect and proposed liberally borrow from GDPR and the Standard Contract Clauses
- Meeting these state laws can assist with GDPR/SCC compliance

Example

- SCC Processor Provisions: New York SHIELD Act of 2019, New York Department of Financial Services Cybersecurity Regulations, California Consumer Privacy Act (“Service Provider”)

Further Examples

- Definitions of Protected Personal Information Expanded: Illinois, California, New York, HIPAA (federal) comprise biometric information, geolocation, device identifiers.
- California Privacy Rights Act will protect trade union membership information and information regarding “philosophical beliefs.”

Practicalities: Think “Business Needs”

Help your US clients get budget for data protection:

1. US state law compliance is necessary for a significant part of the business and compliance representations are in most service agreements
2. Meeting state law common data protection themes accomplishes much of what GDPR requires

Practicalities (cont'd)

3. Expansion to EU is simpler and less expensive if the data protection foundation has been laid with state law compliance. The EU may recover economically at a faster pace than the US and EU customers and business partners insist on strong data protection.

WHAT BREXIT MEANS FOR U.K. DATA PROTECTION

17



Kim Roberts
King & Spalding
125 Old Broad Street
London, United Kingdom
EC2N 1AR
kroberts@kslaw.com
+44 20 7551 2133

THE TRANSITION PERIOD

18

- The U.K. left the European Union on 31 January 2020
- The period until the end of 2020 is a transition period during which the U.K. and the EU will negotiate trade deals
- During the Transition Period the status quo will remain
 - GDPR and national law remains unchanged in the U.K.
 - Data transfers can continue to be managed under the existing framework



2021 AND BEYOND

19

- GDPR will not apply after the Transition Period
- The U.K. has implemented national law (The Data Protection Act 2018 “DPA”) which mirrors GDPR
- The provisions of GDPR will be incorporated directly into U.K. law from the end of the transition period, and will sit alongside the DPA



2021 AND BEYOND

20

- In practice there will be no change to the application of core principles of existing data protection law to the U.K. after the Transition Period
- However, much depends on the nature of the deal negotiated between the U.K. and the EU, in particular how the position on data transfers from the EEA to the U.K. will be resolved



2021 AND BEYOND

21

- Whilst the U.K.'s position is subject to ongoing negotiations, the Information Commissioner's Office (ICO) has confirmed that the default position will be the 'no-deal' position
- After the end of the Brexit long stop date, GDPR will no longer be applicable in the U.K.. Implementing legislation has been enacted to incorporate a version of GDPR (the U.K. GDPR) into U.K. law



SCOPE OF U.K. GDPR

22

- Mirroring the extra territorial scope provisions in GDPR, U.K. GDPR will apply to controllers and processors based outside the U.K. if their processing activities relate to:
 - offering goods or services to individuals in the U.K.; or
 - monitoring the behaviour of individuals taking place in the U.K.



DATA TRANSFERS AND BREXIT (1)

23

- At the end of the transition period there will be two sets of rules to consider:
 - U.K. rules on transferring data out of the U.K.
 - Impact of EU transfer rules on transfer from outside the U.K. (including data transfers from the EEA) into the U.K.



DATA TRANSFERS AND BREXIT (2)

24

- U.K. GDPR restricts transfers of personal data from the U.K. to countries outside the U.K. in the same way as restricts transfers from the EEA

- Lawful transfers can be made if covered by:
 - an adequacy decision
 - an appropriate safeguard (standard contractual clauses, Binding Corporate Rules)
 - the same exceptions as apply under GDPR



DATA TRANSFERS AND BREXIT (3)

25

- GDPR restricts transfers of personal data from the EEA to “third countries”
- From 1 January 2021 the UK will be considered to be a third country.

- Lawful transfers can be made if covered by:
 - an adequacy decision
 - an appropriate safeguard (standard contractual clauses, Binding Corporate Rules)
 - the exceptions under GDPR



U.K. AND ADEQUACY

26

- U.K. is currently undergoing an adequacy assessment by the EU
- No decision as to whether the U.K. will be deemed to be an adequate jurisdiction
- EU has expressed concerns over the U.K.'s surveillance rights and powers as a reason why U.K. may not be considered to be an adequate jurisdiction
- Transfers from adequate jurisdictions (such as Canada, New Zealand, Japan, Israel) to the U.K. may continue, if the U.K. agrees reciprocity with respect to these jurisdictions



EU REPRESENTATIVES AND DPO'S

27

- After Brexit U.K. businesses which do not have a branch, office or other establishment in any other EU or EEA state, but which either:
 - offer goods or services to individuals in the EEA; or
 - monitor the behaviour of individuals in the EEA,still need to comply with GDPR rules on appointing a representative in the EU or EEA state where the individuals whose personal data is processed are located
- The requirement is subject to the exception: “occasional processing” and “low risk” processing
- Ongoing requirement to have a DPO under U.K. GDPR
DPO may cover the U.K. and EEA if ‘easily accessible from each establishment’ in the EEA and U.K.



LEAD SUPERVISORY AUTHORITY

28

- ❑ One Stop Shop mechanism in GDPR will no longer apply to the U.K.
- ❑ U.K. businesses which process personal data of EU nationals may need to recognize more than one supervisory authority
- ❑ Assess the processing activity, geographical location of the business and where the individuals whose data is being processed are located
- ❑ ICO intends to continue cooperation with EU regulators with respect to various matters including data breaches which impact individuals across the EU



PRACTICAL STEPS

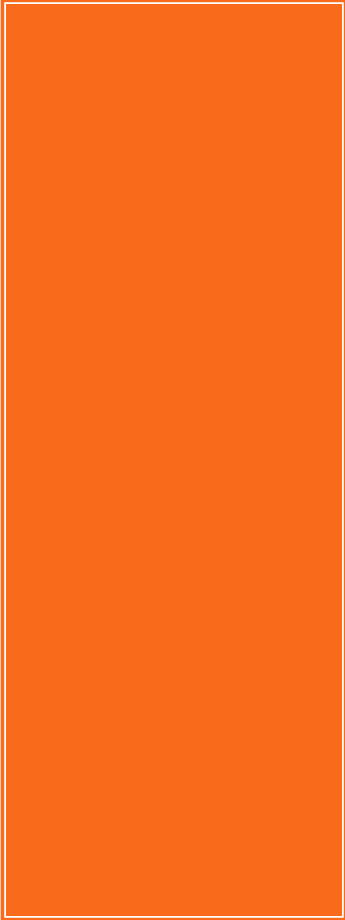
29

- Assess adequacy of current relationships and the changes which may be required to ensure that international data transfers are lawful and correctly documented
- Changes may be required to fair processing notices and policies such as employee notices and online privacy policies
- Data mapping and Article 30 record of processing should be checked with respect to data flows and amended where required



Insights for Building a Global Privacy Program from a Chief Privacy Officer

30



Nick Oldham
Chief Privacy & Data Governance Officer
Equifax Inc.
Atlanta, Georgia
Nicholas.Oldham@equifax.com

Overview

31

- Globalization of Privacy Requirements
- Components of a Global Privacy Program
 - 4 C's:
 - Culture
 - Controls
 - Compliance
 - Communication

Global privacy programs should be globally aligned, locally deployed, and organizationally measured, using the 4 Cs as the guiding principles.

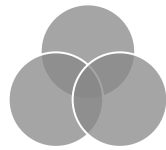
Globalization of Privacy Requirements

32

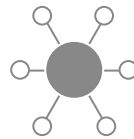
- Each new privacy law or regulation has many core **common compliance requirements**, but the scope of those requirements vary based on different views on what a person's rights are when it comes to privacy.
- The number of privacy laws and regulations are **growing and evolving**, making compliance particularly challenging for multinational organizations.
- Organizations, especially multinational organizations, should align their privacy programs around a **control framework** to meet their growing and evolving privacy requirements.

Components of a Global Privacy Program

33



GLOBALLY
ALIGNED



LOCALLY
DEPLOYED



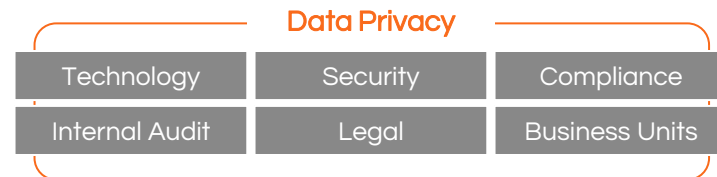
ORGANIZATIONALLY
MEASURED

The program is centered around 4 key concepts:

The
4 C's

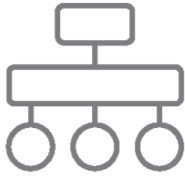
1. Culture
2. Controls
3. Compliance
4. Communication

Internal partners are used to incorporate privacy throughout the business



Privacy Program: Culture

34



Influence

Privacy must have sufficient visibility within the organization



Ingrain

Privacy is built into each phase of application design, development, and operation



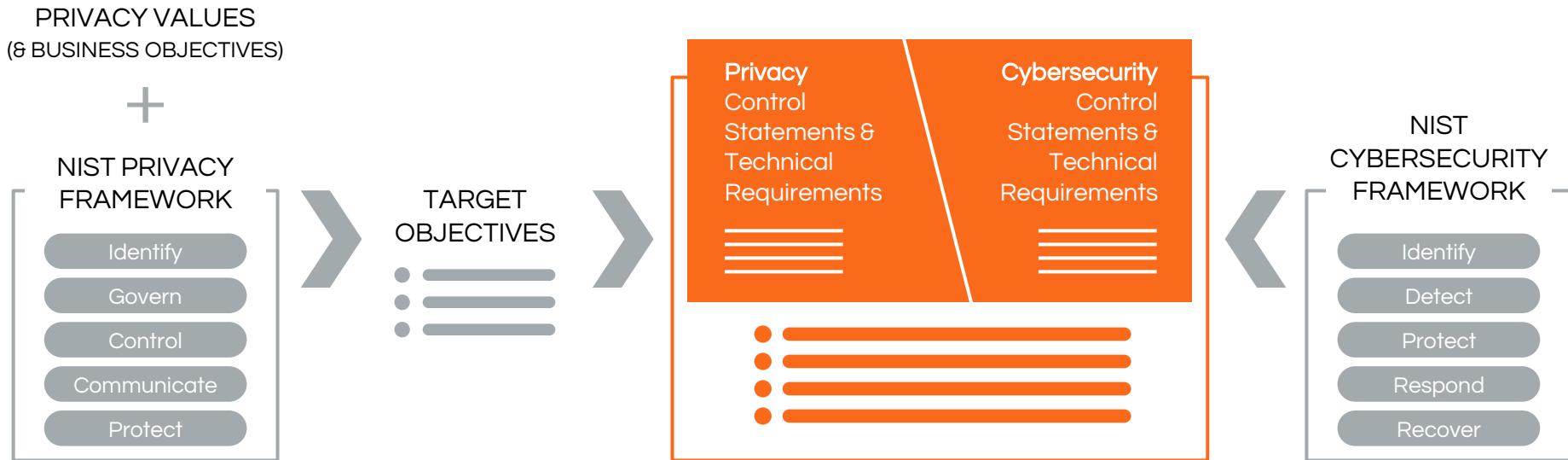
Incentives

Privacy milestones incorporated into enterprise-level incentives

Privacy Program: Controls

35

Drafting Privacy Controls



NIST Privacy Framework Alignment Example

36

KEY CONSIDERATIONS

1. Current security program framework
2. Privacy program maturity
3. Enterprise Privacy Values

HELPFUL FACTORS

1. NIST CSF alignment
 - Common framework structure
 - Mapping between security and privacy controls

SCENARIOS

In general, there are three scenarios for aligning the NIST PF into an established control framework:

- 1 **Revisions** to existing controls (through additional Technical Requirements or modifications to existing language)
- 2 **Net new** controls (beyond the scope of the NIST CSF)
- 3 Existing controls without need for modification

Privacy Framework Implementation Example

Updates to Current Controls and Technical Requirements (Illustrative)

Privacy Framework

GV.RM-P2
Organizational risk tolerance is determined and clearly expressed.

GV.RM-P3
The organization's determination of risk tolerance is informed by its role in the data processing ecosystem.

Cybersecurity Framework

ID.RM-2
Organizational risk tolerance is determined and clearly expressed

ID.RM-3
The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis

Control Statement

RSK-CS-2: The Company's Board of Directors reviews and approves the organization's risk appetite, Enterprise Security Risk Assessment, **Enterprise Privacy Risk Assessment**, Enterprise Threat Vector Assessment, Asset Criticality Risk Assessment, and the Security Risk Methodology on a periodic basis.

RSK-CS-10: Company performs an Enterprise Privacy Risk Assessment to assess the internal and external risks to the processing of personal data on a periodic basis.

Technical Requirements

RSK-TR-21: Company designs, implements, maintains, and documents safeguards that mitigate the material internal and external risks Company identifies to the privacy of personal data.

KPI Examples:

- % - risks remediated within SLA according to remediation plan
- % - open criticals and highs as a percent of total issues
- % - controls operating without a variance

Privacy Framework Implementation Example

Net New Technical Requirements (Illustrative)

Privacy Framework

Cybersecurity Framework

Control Statement

CT.PO-P1:
Policies, processes, and procedures for authorizing data processing (e.g., organizational decisions, individual consent), revoking authorizations, and maintaining authorizations are established and in place.

N/A

GOV-CS-11: A global privacy program based on company-wide privacy principles and a privacy charter is formally defined, documented, and implemented.

Technical Requirements

GOV-TR-17.2: The Company Privacy Program includes regional Policies, Procedures, Processes and Training, as appropriate.

CT.PO-P2:
Policies, processes, and procedures for enabling data review, transfer, sharing or disclosure, alteration, and deletion are established and in place.

N/A

GOV-TR-17.2.1: Company publishes, as appropriate, updated Policies, Procedures, Processes and Training to readily accessible locations and communicates the updates to Employees and relevant third party stakeholders.

GOV-TR-20: Company maintains an Acceptable Data Use process, including a policy and process for authorizing, revoking and maintaining data processing activities and enabling data review, transfer and sharing.

GOV-TR-21: Company maintains a Privacy by Design process, including defined requirements for data manageability and privacy that must be implemented during the System Development Life Cycle (SDLC).

Key KPI Examples:

% of Data Uses reviewed within SLA via the Acceptable Data Use process

% of products meeting Privacy by Design requirements

% of governance documents reviewed and reissued per SLA

Privacy Program: Compliance

39

Transactional compliance is not scalable

The goal should be organizational compliance through appropriate processes and controls that can be measured to show success



Privacy Program: Communication

40

Appropriate
Process



Proven
Execution



Trust In The
Program



Privacy
Principles



Measurable
Progress



Internal
Stakeholders



External
Stakeholders

Questions

Walt Saprnov



42

770.399.9100
wsaprnov@wstelecomlaw.com



Walt Saprnov has represented corporate clients in telecom transactions, regulation and privacy for over thirty years. He has been named in Georgia Super Lawyers and in the International Who's Who of Telecom Lawyers. Together with his Firm, Saprnov & Associates, P.C., he has negotiated commercial telecom contracts with every major telecom carrier in the U.S. and with many abroad. The Firm also supports clients in privacy compliance before the FCC, the FTC, EU and state regulatory agencies. Mr. Saprnov is a frequent conference speaker and has authored numerous publications on telecommunications law.

For more information, please visit:
www.wstelecomlaw.com

Joseph Srouji



43

Mr. Srouji, based in Paris, France, is Of Counsel to Sapronov & Associates, P.C. and Founding Partner of Srouji Avocats. He is former Senior Counsel for Data Protection & Regulatory Affairs at GE Capital where he worked for over 11 years based in Paris as a specialist in data protection, financial and banking regulation and compliance.

He teaches International Law and Technology Law to graduate students at Université Paris II Panthéon – Assas. He is a member of the Paris Bar and certified CIPP-E.



jsrouji@wstelecomlaw.com
222 Boulevard Saint Germain
75007 Paris - France
+33 (0) 1 78 64 64 83

Kenneth N. Rashbaum

BARTON
Discover Better Law

44

Kenneth N. Rashbaum advises multinational corporations and healthcare organizations in the areas of privacy, technology transactions and e-discovery. He counsels these organizations on information management and its compliance with federal, state, and non-U.S. laws. Ken also prepares and negotiates contracts and license agreements for financial services, technology and e-commerce companies and advises clients on cyber risk insurance and other information use safeguards. He is experienced in preparation of protocols for compliance with data protection and privacy laws in the U.S. and other countries and conduct of information security and data breach response assessments, and investigations and remediation initiatives. Ken has worked with the New Jersey legislature on drafts of proposed data protection legislation has served as national e-discovery counsel for multinational pharmaceutical corporations and global e-discovery counsel in products liability and IP litigation. A prolific speaker and writer on privacy and cybersecurity, Ken is also an Adjunct Professor of Law at Fordham Law School, an officer of the International Law Section of the American Bar Association and a Fellow of the American Bar Foundation. Prior to joining Barton, Ken was a senior litigation partner and founding co-chair of the cybersecurity practice at Sedgwick LLP (formerly Sedgwick, Detert, Moran and Arnold).



krashbaum@bartonesq.com
212.885.8836

Kim Roberts



45

Kim Roberts represents global corporates and large employers on their employment law and data privacy strategy in the U.K. and across Europe. She has particular experience with international clients headquartered outside the U.K., specifically those in the U.S. with global operations.

Kim advises on data protection and privacy issues. She specializes in advising cross border European clients on their data privacy obligations, data privacy policies and employee data management. Kim advises clients on developing law and practice in the EU including the GDPR, and on obligations when transferring data between the EU and the U.S., including advice on Model Clauses and the EU/U.S. Privacy Shield.

Kim speaks regularly at client events and seminars and commentates in the U.K. national press on employment law and data privacy matters and developments.



**44 (0) 20 7551 2133
kroberts@kslaw.com**

Nicholas Oldham

46

Nick Oldham is Equifax's Global Chief Privacy and Data Governance Officer, leading a privacy and data governance organization that functions at the intersection of privacy and security with enterprise-wide responsibility for strategy, policy, and operations. He is responsible for privacy controls holistically. In addition to traditional privacy controls, he is also responsible for data controls like DLP, data discovery, records retention, and acceptable data use.

Nick is a lawyer by training and spent several years in both the government and private practice. A former federal criminal prosecutor, Nick spent more than seven years with the U.S. Department of Justice, where he handled high-profile cyber investigations and prosecutions, and served as the first Counsel for Cyber Investigations for the DOJ's National Security Division. While at King & Spalding in Washington, D.C., Nick helped clients build and improve their controls around cybersecurity, privacy, and data use.



Nicholas.Oldham@equifax.com