



**UNIVERSITÉ  
RENNES 2**



ALLIANCE  
SORBONNE  
UNIVERSITÉ



**utc**



# Data Protection Law 101

**Julien Rossi**

**julien.rossi@univ-rennes2.fr**  
**@julienrossi**

**julien.rossi@univ-rennes2.fr**

**Twitter: @julienrossi**  
**www.julienrossi.com**

# The GDPR

- What do you know about it?
- When and how did you hear about it?
- What country/jurisdiction are you from?

**Where does the GDPR come from?**



Allianz



Allianz  
Conduite  
connectée

avec la technologie **TOMTOM**



TOP SECRET//SI//ORCON//NOFORN



Hotmail



AOL mail



(TS//SI//NF) **PRISM Collection Details**



Current Providers

What Will You Receive in Collection  
(Surveillance and Stored Comms)?  
It varies by provider. In general:

- Microsoft (Hotmail, etc.)
- Google
- Yahoo!
- Facebook
- PalTalk
- YouTube
- Skype
- AOL
- Apple



- E-mail
- Chat – video, voice
- Videos
- Photos
- Stored data
- VoIP
- File transfers
- Video Conferencing
- Notifications of target activity – logins, etc.
- Online Social Networking details
- **Special Requests**

Complete list and details on PRISM web page:  
Go PRISMFAA

TOP SECRET//SI//ORCON//NOFORN



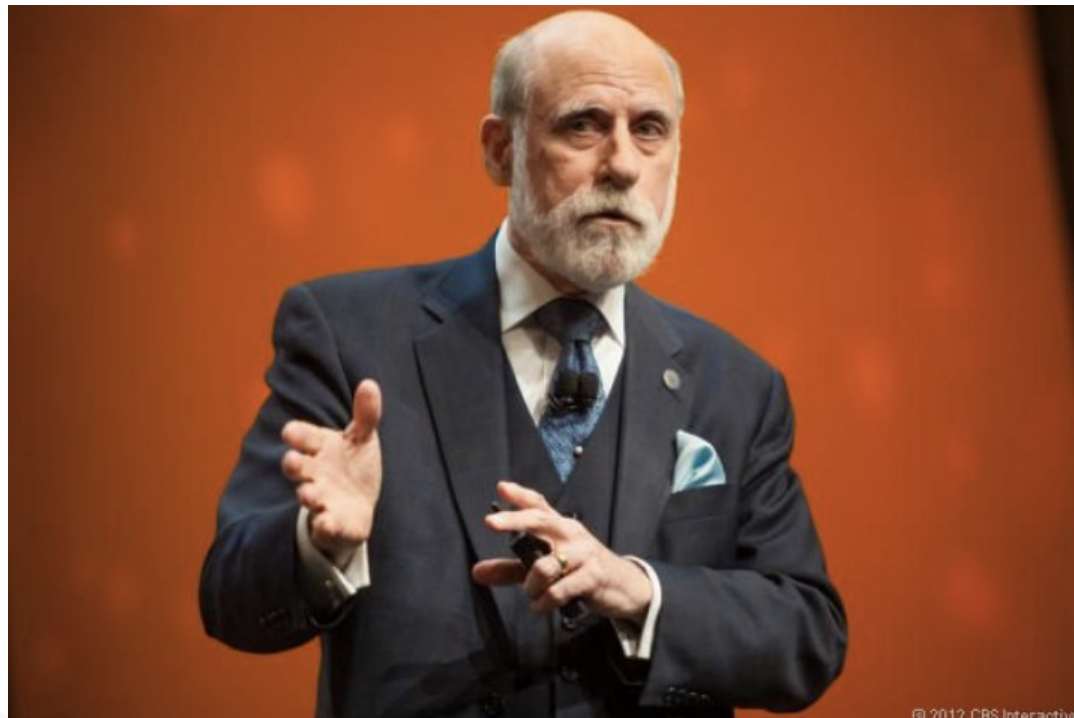
# Is he right?

SECURITY

## Vint Cerf: 'Privacy may be an anomaly'

The so-dubbed father of the Internet believes privacy will be increasingly harder to achieve given our desire to tell all via social media.

BY LANCE WHITNEY | NOVEMBER 20, 2013 5:34 AM PST



<https://www.cnet.com/news/vint-cerf-privacy-may-be-an-anomaly/>

# What's privacy to begin with?

- **Samuel Warren & Louis Brandeis (1890):** it's the "right to be let alone"
- **Irwin Altan (1977):** privacy is a universal need, but the needs has culturally relative manifestations
- **Bénédicte Rey (2009):** privacy, from a sociological point of view, could be defined as a reaction to a feeling of intrusion
- **Helen Nissenbaum (2010):** privacy is *contextual*
- **Deirdre Mulligan, Nick Doty & Colin Koopman (2016):** privacy is an *essentially contested notion*
- **Koops et al. (2016):** how about we answer the question by looking at what privacy law protects?

# **A fundamental right**

- **Art. 8 ECHR**
- **Art. 7 & 8 of the EU's Charter of Fundamental Rights**

**Okay, that's great.**

**But where does the term “data protection” come from?**

# Timeline

- **Early 1960's: plans for a National Data Center in the United States**
  - Similar plans are made in Europe
  - Early digitisation of public administrations
- **1966: first mention of the “right to be forgotten”, in the U.S.**
- **1970: Hessisches Datenschutzgesetz**
- **1978: French Data Protection Act**
- **1981: Convention 108**
- **1995: Data Protection Directive (95/46/EC)**
- **2016: Regulation 2016/679/EU and Directive 2016/680/EU**

**Wait, what?**

**1960's?**

**So the GDPR wasn't the end of the  
world as we knew it?**

« I have become convinced that the magnitude of the problem we now confront is akin to the changes wrought in our national life with the dawning of the nuclear age »

— Frank Norton

Cornelius Gallagher: « The possible future storage and regrouping of such personal information also strikes at the core of our Judeo-Christian concept of “forgive and forget,” because the computer neither forgives nor forgets. »

4. G 74/1: 13/2

---

**THE COMPUTER AND INVASION OF PRIVACY**

---

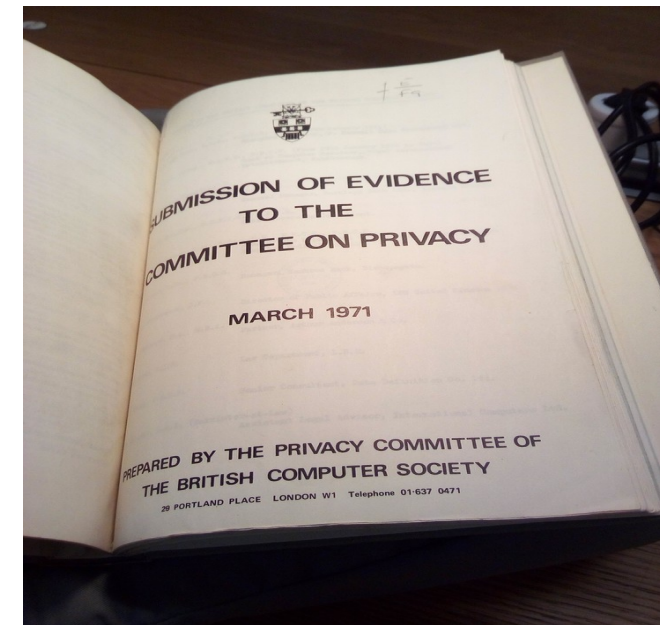
DOCUMENTS  
ROOM

Y4.G74/7:  
P93/2

**HEARINGS**  
BEFORE A  
SUBCOMMITTEE OF THE  
COMMITTEE ON  
GOVERNMENT OPERATIONS  
HOUSE OF REPRESENTATIVES  
EIGHTY-NINTH CONGRESS  
SECOND SESSION

JULY 26, 27, AND 28, 1966

Printed for the use of the  
Committee on Government Operations



**STATEMENT OF PAUL BARAN, COMPUTER EXPERT WITH THE  
RAND CORP., SANTA MONICA, CALIF.**

Mr. BARAN. Thank you, Mr. Chairman. I would first like to summarize my remarks and then delve more deeply into the reasons for my position. I do so in the role of the private citizen and not as a representative of the Rand Corp. or its sponsors.

Recommendation 509  
on Human Rights and Modern Scientific and Technological  
Developments (Draft Programme of Work,  
1968/69, Chapter II(1))

---

Memorandum submitted by the Secretariat

---

1. The Ministers' Deputies, at their 168th meeting in March 1968, considered the Assembly's Recommendation 509 proposing that a study should be made of the question whether, having regard to Article 8 of the Convention on Human Rights, the national legislation in member states adequately protects the right to privacy against violations which may be committed by the use of modern scientific and technical methods. The Assembly also urges that, if the answer to this question is in the negative, recommendations should be made for the better protection of the right to privacy. At the conclusion of the discussion, the Secretariat was instructed to prepare a paper which would, first, establish the facts and define the problem; then consider what action is required and what is the most appropriate body to undertake it.  
(CH/Del/Concl. (68) 168, point III, A (d)).

This document has been prepared by the Secretariat in accordance with these instructions.

# Spiros Simitis

**« When we started thinking about that, and discussing it, and trying to react to it, one of the main sources of our reflection and of our expectations, was a continuous study on decisions, court decisions, in the United States, that had already to do with automation. The Americans themselves had not yet a law. But they offered most of the material, because the automation in their industry for instance was by far more developed than in Europe. So the ... the strange particular thing, one the one side of the Ocean you had the Americans with the automation and continuously new forms and developments. And on the other side of the Ocean, you had people who [...] for the first time realised you could not accept the consequences of a supposed objectivity because the data were processed automatically. »**

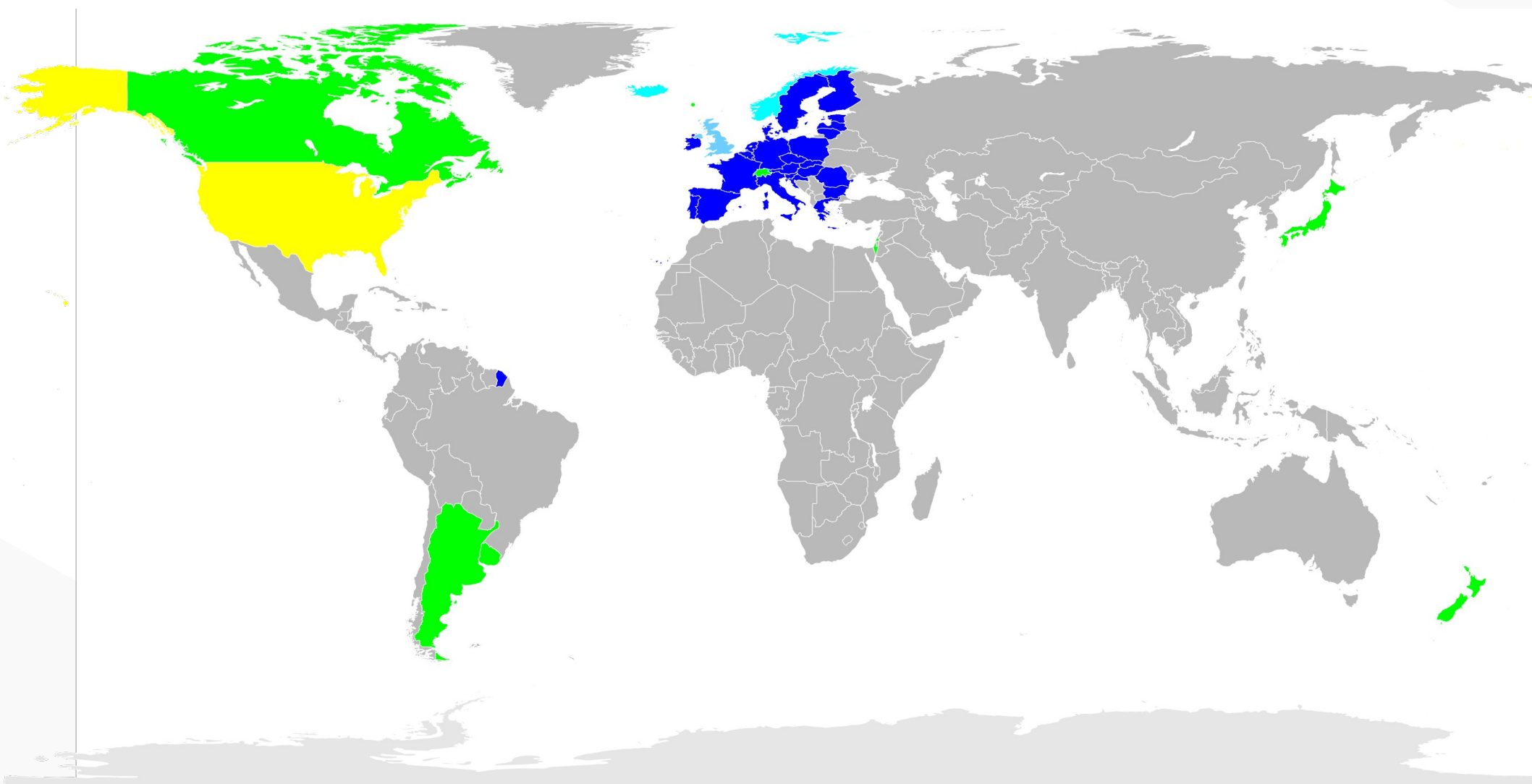
**- Spiros Simitis, interview**

39. PRINCIPLE NO. 1 - The information should be regarded as having been provided for a specific purpose, and without appropriate authorisation it should not be used for other purposes, or communicated to third parties without the agreement of the person concerned.
40. PRINCIPLE NO. 2 - Access to the information stored should be confined to persons who can establish a valid reason in obtaining the information.
41. PRINCIPLE NO. 3 - Information should not be stored if it is irrelevant or to an amount excessive according to the given purpose.
42. PRINCIPLE NO. 4 - Statistical data may only be published in aggregate form and under conditions which will make it impossible to reconstitute information so as to permit the identification of individuals.
43. PRINCIPLE NO. 5 - Measures should be taken in order to inform the person concerned of the nature of the information held about him, and if possible of the purposes for which the information will be used.

**The GDPR was announced in 2009 ...**

**... but first, let's talk about techno-  
policy standards (Mulligan & Doty,  
2013) ...**

**... and then a bit about how the rules  
laid down in Convention 108 and  
Directive 95/46/EC spread across the  
world ...**



**... now we can go back to the GDPR.**

# A brief history of the GDPR

- **Well, there was actually a movie made about it...**
  - > [trailer](#)
- **Discussions started with consultations by the EU Commission in 2009**
- **In 2012, the Commission published its proposal**
- **In 2016 it was finally adopted by the Council of the EU and the European Parliament**
- **It entered into force last year on the 25<sup>th</sup> of May**

# Scope of application

- **Material** :

- Art. 2 §1 : “This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system”
- Exceptions: domestic use, police & criminal justice (Directive 2016/680/EU), and anything outside of EU law

- **Territorial** :

- 1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.
- 2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
  - (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
  - (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.
- 3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

# Definitions

- **Let's take a look at article 4, and define:**
  - **Personal data**
    - **Special categories of personal data => article 9**
    - **Some examples**
  - **Data subject**
  - **Pseudonymisation (vs. anonymisation)**
  - **Data processing**
  - **Data controller**
  - **Data processor**
  - **Recipient**

# Principles

- **Article 5**
  - **Lawfulness, fairness and transparency**
  - **Purpose limitation**
  - **Data minimisation**
  - **Accuracy**
  - **Storage limitation**
  - **Integrity and confidentiality (aka security)**
  - **Accountability**
- **“User participation” (OECD Guidelines ; Chapter III of GDPR)**

# **Legal bases => conditions for lawfulness**

- **Art. 6 §1**

- **Consent**

- **See definition of consent in article 4**
    - **See conditions for consent in article 7**
    - **Cookie consent => it's also in 2002/58/EC, art. 5 §3**
      - **See : ECJ, 1<sup>st</sup> October 2019, “Planet 49”, Case C-673/17**

- **Contract**

- **Compliance with legal obligations**

- **Protecting vital interests of someone**

- **Task carried out in the public interest or in the exercise of official authority**

- **Legitimate interest of the data controller or a third party**

- **Legitimate interest => it creates the possibility of opt-out**

# Rights of data subjects

- **Data subject rights are covered by Chapter III of the GDPR**
- **They include :**
  - The right to information (be transparent) (art. 12 to 14)
  - The right to object (when processing is based on “legitimate interest”) (art. 21)
  - The right to access (free of charge) (art. 15)
  - The right to rectification (art. 16)
  - The right to erasure (aka. “right to be forgotten) (art. 17)
  - The right to data portability (art. 20)
  - The right “not to be subject to to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her” (art. 22)
- **A significant number of fines recently decided by DPA’s could have easily been avoided by having at least attempted to implement processes to comply with such data subject requests!**

**Where to look for some further  
information**

Let's start with the basics.

- [The GDPR](#), the one and only
- [Directive 2016/680/EU](#) (should you ever work for Police or Justice departments, you should know that one too)
- [Regulation 2018/1725/EU](#) (that is for if you ever work for the EU; it applies data protection law to the EU institutions themselves)
- [Directive 2002/58/EC, 2009 edition](#), (aka the e-Privacy directive, aka the EU Cookie Law, even though it's actually about much more than just cookies)

You can also check out your DPA's website. If you are French, you can visit the website of Commission nationale de l'informatique et des libertés @ [www.cnil.fr](http://www.cnil.fr)

Check out if your country has a national association of Data Protection Officers too. In France, there is [AFCDP](#). In the Netherlands, [NGFG](#). In Romania, there is the [ASCPD](#). On an international level, check out the [IAPP](#). Etc.

- [Handbook on European data protection law, 2018 edition](#), by the Fundamental Rights Agency of the EU. As Donald Trump would say: it's a **tremendous** book. On a more serious note: I truly recommend it as a guide on this topic. It's free, but very high quality nonetheless, and quite well explained.
- If you want to know more about what European Data Protection Authorities have to say on a wide range of topics, check out [the website of the European Data Protection Board](#) for guidance. Its ancestor, [the Article 29 Working Party](#), also published opinions and guidelines that – for most of them – are still valuable.
- [GDPR Today](#). Yes, the GDPR has its own newspaper. No it's not a real newspaper, but it does provide a great selection of news articles related to the GDPR, which is updated on a regular basis by an NGO called European Digital Rights, to whom we owe a lot of what ended up in the GDPR.

- Computers, Privacy and Data Protection. Every year, this conference brings over a thousand data protection geeks from all over the world in Brussels for a weekly marathon of exhibitions, all-night-long partying, networking and some serious beer-tasting. Oh and also a lot of usually good quality talks and panels that [are all uploaded onto Youtube](#), so that you can fill your time while the world is on shutdown because of Coronavirus. If one day you go to CPDP, give me a shout.
- [The GDPR Hub](#). By None Of Your Business, a Vienna-based NGO run by Max Schrems, the guy who took down the Safe Harbor agreement for the free-flow of personal data between the EU and the US in 2015. It includes a lot of resources, commentaries on the Law, information on DPA decisions.
- In terms of standards, you can check out the [Privacy Enhancements and Assessments Research Group](#) @ IETF and the [Privacy Interest Group](#) @ W3C

- If you're looking for some music, [you can check out the playlist by DJ Sœur Veillance](#), who is also a leading expert in data protection law
- If you are looking for some academic articles... it's hard to know where to start. There is so much! But here are some reviews that have generally good articles on topics such as privacy, data protection and surveillance:
  - [Surveillance & Society](#)
  - [European Data Protection Law Review](#)
  - [Internet Policy Review](#)
- There is a lot more... but honestly, it would be difficult to give you a list of all the good articles out there. Or the list would be so long it would scare anyone looking at it from going through it. So if you are looking for some articles on a specific topic, don't be afraid to send me an e-mail

# Exercise

**1. What is the right to be forgotten?  
How does it relate to Google?  
What did the GDPR change?**

**2. What is a privacy policy?  
Which article(s) mandate data  
controllers to have one?  
What should be in it?**