



Πανεπιστήμιο Αιγαίου

# Προστασία Προσωπικών Δεδομένων

## Communications Data Retention and its Impact on Rights and Democracy

Λίλιαν Μήτρου ([L.Mitrou@aegean.gr](mailto:L.Mitrou@aegean.gr))

Αναπληρώτρια Καθηγήτρια

Τμήμα Μηχανικών Πληροφοριακών & Επικοινωνιακών  
Συστημάτων



Ευρωπαϊκή Ένωση  
Ευρωπαϊκό Κοινωνικό Ταμείο



ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ & ΘΡΗΣΚΕΥΜΑΤΩΝ, ΠΟΛΙΤΙΣΜΟΥ & ΑΘΛΗΤΙΣΜΟΥ  
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης



# Άδειες Χρήσης

- Το παρόν εκπαιδευτικό υλικό υπόκειται σε άδειες χρήσης Creative Commons.
- Για εκπαιδευτικό υλικό, όπως εικόνες, που υπόκειται σε άλλου τύπου άδειας χρήσης, η άδεια χρήσης αναφέρεται ρητώς.



# Χρηματοδότηση

- Το παρόν εκπαιδευτικό υλικό έχει αναπτυχθεί στα πλαίσια του εκπαιδευτικού έργου του διδάσκοντα.
- Το έργο «**Ανοικτά Ακαδημαϊκά Μαθήματα στο Πανεπιστήμιο Αιγαίου**» έχει χρηματοδοτήσει μόνο τη αναδιαμόρφωση του εκπαιδευτικού υλικού.
- Το έργο υλοποιείται στο πλαίσιο του Επιχειρησιακού Προγράμματος «Εκπαίδευση και Δια Βίου Μάθηση» και συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση (Ευρωπαϊκό Κοινωνικό Ταμείο) και από εθνικούς πόρους.



Ευρωπαϊκή Ένωση  
Ευρωπαϊκό Κοινωνικό Ταμείο



ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ & ΘΡΗΣΚΕΥΜΑΤΩΝ, ΠΟΛΙΤΙΣΜΟΥ & ΑΘΛΗΤΙΣΜΟΥ  
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης



# The issues

- An answer to “pressing security needs”?
- The context of communication technologies
- Data retention as interference with privacy, freedom of expression and freedom of movement
- Data retention as the negation of proportionality
- Data retention as “democracy risk”

# 11/9 and legislative activism

- Security has always been a point of the regulatory agenda
- A legal framework with “security deficiencies” ?
- Re-introduction of proposals that (previously) had “no chance to be accepted”
- No doubts/justification for the necessity of new regulation
- Attack/Risk as evidence



# Data retention as security tool

- Data relating to the use of communications as a “valuable tool” in the context of prevention, investigation, detection of risk, threat and crime
- Communications data used in order to locate and trace source and route, to collect and secure evidence
- Providers in EU are mandated to retain routinely communications data of any and all subscribers for investigational purposes (Directive 2006/24/EC)

# Mandatory data retention

- Data necessary to identify the “external conditions of communication”
- For the investigation, detection and prosecution of serious crimes (as defined in each MS)
- For a period of 6 months- 2 years
- Accessible in specific cases by the designated authorities



# The technological context

- ICTs require or have as result the exchange of data
- Information is available for scrutiny in ways and volumes unimaginable till now
- Surveillance potential grows wider through ubiquity and integration of ICTs
- ICTs become more interconnective and their use more extensive and intensive



# ...in a technology neutral way...

- Traffic data are covered in a technology-neutral way
- Neutrality: necessary in order to keep pace with changing technological environment
- The use of technology-neutral language ignores the specific challenges and risks

# “Envelop” and content?

- The Data Retention Directive does not allow content monitoring....however...
- In the electronic space the boundaries between communications data and content are blurring
- The ambiguity of distinction is acute in the context of networks
- Data necessary for a communication reveal elements of content  
[www.google.com/sites/web?q=aids+medical+treatment](http://www.google.com/sites/web?q=aids+medical+treatment)
- Informative value/usability of traffic data



# the “traceable past” and the .....foreseeable future?

- Data retention enables the development of models of what is “suspicious communication”
- Networks increase the quantity, quality and accessibility of information relation to online and offline behaviour
- Internet becomes a medium that promotes “relative transparency”
- By exploiting the specific features of ICTs data retention makes past and present traceable and the ...future foreseeable



# Interference with privacy

- Communication with others and use of communications means/services falls within the zone of privacy
- Decisive is that state authorities can access the data retained by private providers
- Seriousness of the interference is to be assessed according to preconditions of power granted, number and nature of individuals affected and intensity of negative effects

# Privacy as element of Democracy

- Freedom of unwarranted and arbitrary interference from public authorities
- The European approach of privacy is grounded on dignity of a person who operates in self-determination as a member of a free society
- Privacy enables individuals to take autonomous decisions, to build social appearance and behavior, to develop their own identity and ideas in order to engage in relationships with others and in public life
- A key element of a democratic constitutional order and fundamental political value



# Anonymity as element of Democracy

- As electronic communications leave a lot of “traces” surveillance has disturbing effects on the right to anonymity
- Anonymity helps information and ideas to be disseminated and considered without bias, to voice critical ideas
- Anonymous speech has an instrumental value in enriching public discussion and maximizing freedom of association
- “Chilling effect”: concern that constitutionally protected activity would be inhibited due to the fear of post-hoc surveillance



# Freedom of movement

- Data retention as the disappearance of the disappearance
- The freedom of movement concerns also the right to move without being traced
- Networks transform the notions of “place” and “space”
- As many users live their life in cyberspace freedom of movement can be considered as affected.

# The negation of proportionality/1

- State powers to limit freedom were addressed at the person causing the “danger”, the “disturber”, the “suspect”
- Now surveillance is extended to cover the majority of population
- Data retention enables the permanent, general recording of communicational behavior of all subscribers, although neither they are neither a “source of danger” nor their communications take place in an unusually dangerous area



# The negation of proportionality/2

- Constitutional intervention in rights and liberties is subject to the principle of proportionality (ban on undue intervention) : Necessity, suitability to achieve aims, scale – intensiveness
- Data retention without to demonstrate that this large-scale surveillance potential was the only feasible option
- Security as “self-evident fact”: as such it cannot be understood in a normative sense
- Data retention is so extensive as to be out of all proportion



# “an extended logbook” ?

- Considering the increased use of electronic communication means and services and the amount of information which can be revealed and stored
- the retention of communications data is a “serious interference into the freedom of communication that cannot be undone, as such an access enable far reaching insights into the behavior and the social contacts of individuals” (German Federal Constitutional Court, March 08)

# Surveillance as rule/norm

- Indefinite and ongoing interference with the communicational privacy of all users for reasons of precaution makes surveillance the rule
- It shifts the focus of risk from suspect individuals to suspect populations
- It shifts the "burden of proof": the state is often not obliged to demonstrate individualized suspicion in order to target individuals
- Every person a potential source of risk/criminal



# Dataveillance

- Data are gathered not occasionally but via routinized discovery systems
- The retention of data on citizen's behaviour and social interaction may shape and steer this behaviour , "as people act differently if they know their conduct could be observed" (US Department of Defense, 2004) and tend to incline their choices to the mainstream
- The "maximum security society" relies on a refined technological framework to influence and "programme" the daily life

# The “security promise”

- Security has emerged not only as the state’s task of guaranteeing constitutionally protected freedoms
- Security as the (new?) normative guiding principle – the development of the “protection duties” is of central importance for the extended justification of rights infringements
- Collective security goods on the same level with individual civil liberties
- A new fundamental “right to security”?



# Pre-prevention at random

- Shift from a constitutional state guarding against the threat of specific risks in specific situations toward a pre-preventive state
- Dissociation of risk and individual acts and focus on risk prevention
- Shift from the traditional constitutional model of gathering conclusive evidence of suspect individuals toward intelligence gathering carried out against individuals at random

# De-individualisation of freedom?

- Individual rights are replaced by collective interests
- Underlying argumentation: the individual shares its liberal status and has to accept interference in her fundamental rights in order to secure societal freedom
- Affirmative duties lead to a disequilibrium in the balancing process - under the terms and within the limits of core democratic values
- The political impact of the power to obtain such a broad range of information should be taken into consideration – concentration of power



# Data sharing with private sector

- Data retention as a paradigm of increased data sharing between public and private domain
- A broad common information “pool”?
- Function creep and mission creep, which can chill personal and professional activities

# Democratic rights free-zone?

- Democracy is founded on free expression and participation
- Transmutation of communication activity to data routinely retained may discourage civil participation
- Data retention threatens deliberative democracy by inhibiting individuals from engaging in democratic activities