Privacy, GDPR, and the Internet Protocol: When layer 8 meets Layer 3!

Luigi Iannone

PEARG @ IETF 113

Outline

- History Terminology
- GDPR & IP Addresses
- GDPR & IETF Standards
  - Annex A: RFC 8280 - Human Right Protocol Considerations
  - Annex B: RFC 6973 - Privacy Considerations for Internet Protocols

History & Terminology

History of GDPR: General Data Protection Regulation

- Replaces Data Protection Act 1998
- Effective from May 2018
- Its’ a “Regulation” formed by:
    - Articles: the law itself
    - Recitals: explanatory note within the body of GDPR

Personal Data

- **“Personal Data”** means *any information about an identified or identifiable natural person* regardless of whether it is held in paper, electronic or any other format, including:
    - **Identification Data:** e.g. name, personal address, personal telephone number, personal e-mail address, date of birth, national insurance number, photograph, marital status and emergency contact information;
    - **Information concerning employment:** e.g. salary, work and compensation history, planned salary, earnings, career development, paid time off, salary grade, performance information (including appraisals, internal communications, attendance records…), CV…;
    - **Financial information:** e.g. bank account number, tax-related information, salary information;
    - **Sensitive personal information:** e.g. information which may reveal race or ethnic origin, religious or philosophical beliefs, politic opinion trade union membership or data that concerns health or sexual orientation;
    - **other information:** necessary for Huawei’s business purposes which may be voluntarily disclosed by individuals during an employment with Huawei.

Processing & Controlling Personal Data

- **"Controller"** means the *natural or legal person*, public authority, agency or any other body which alone or jointly with others *determines the purposes and means of the processing* of personal data.

- **"Processor"** means a *natural or legal person*, public authority, agency or any other body which *processes* personal data on behalf of the controller.

- **“Processing”** means any *operation* or set of operations that are performed upon Personal Data, whether done by automatic means or otherwise. It includes collecting, recording, storing, organizing, adapting, altering, retrieving, consulting, *using,* disclosing or making available, destroying and/or deleting *personal data*.

GDPR and IP Addresses (and more)

Can a dynamic IP address constitute personal data?

- In the General Data Protection Regulation ("GDPR") that IP addresses should be considered as personal data as the text includes "online identifier", in the definition of "personal data".
- The usual **rules relating to personal data** under current EU data protection law (and certainly under the GDPR) **should be applied to IP addresses**, e.g. controllers must inform users they hold this information, they must tell them why, they must allow them access to this data etc. If website providers can avoid holding IP addresses, or limit them in some way, for example by removing the final octet from the IP address and thereby removing the link to the user's device, this will help, certainly in relation to the security requirements under the current Directive and most importantly under the GDPR.

Principles of Data Processing: Layer 8 vs Layer 3

- An IP Layer and ISP Perspective*

1. LAWFULNESS, FAIRNESS AND T

2. PURPOSE LIMITATION

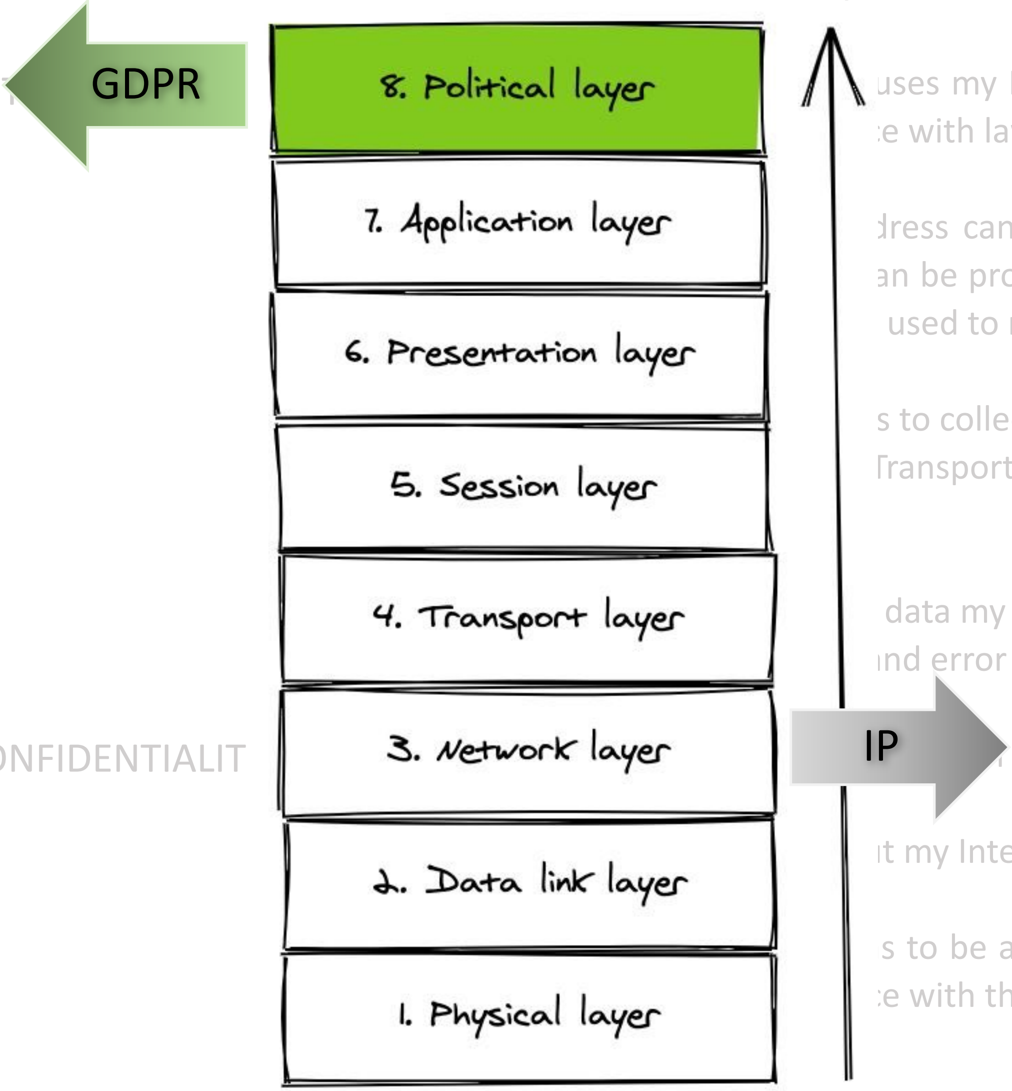
3. DATA MINIMIZATION

4. ACCURACY

5. STORAGE LIMITATION

6. SECURITY (INTEGRITY AND CONFIDENTIALIT

7. ACCOUNTABILITY



uses my IP address for providing Internet Service this must be in
:e with laws and with my consent.

dress can be used to count packets to/from me for billing. This
an be processed for aggregated statistics about network usage. It
used to measure how much shopping I do online.

s to collect only data that are necessary to assure Internet Service
Transport header) but access the content of my packets is against

data my ISP uses to provide me with Internet Service, it has to be
ınd error free.

store my CDR[1] logs only for a limited amount of time.

ıt my Internet usage has to be kept secure and confidential.

s to be able to prove that any data processing has been done in
:e with the laws (GDPR).

* This is personal interpretation and I am not a lawyer

[1] Call Detail Record: https://en.wikipedia.org/wiki/Call_detail_record

Principles of Data Processing: Layer 8 vs Layer 3

1. LAWFULNESS, FAIRNESS AND TRANSPARENCY
2. PURPOSE LIMITATION
3. DATA MINIMIZATION
4. ACCURACY
5. STORAGE LIMITATION
6. SECURITY (INTEGRITY AND CONFIDENTIALITY)
7. ACCOUNTABILITY

- An IP Layer and ISP Perspective*

1. If my ISP uses my IP address for providing Internet Service this must be in accordance with laws and with my consent in a non discriminatory manner.
2. My IP address can be used to count packets to/from me for billing. This number can be processed for aggregated statistics about network usage. It cannot be used to measure how much shopping I do online.
3. My ISP has to collect only data that are necessary to assure Internet Service (e.g. IP + Transport header) but access the content of my packets is against GDPR.
4. Any information my ISP uses to provide me with Internet Service, it has to be accurate and error free.
5. Any information my ISP collects about my IP address can be archived/ stored only for a (predefined) limited amount of time.
6. Data about my Internet usage has to be kept secure and confidential.
7. My ISP shall be responsible for any personal data it is collecting and shall be able to demonstrate that personal data has been processed in accordance with above listed principles.

* This is personal interpretation and I am not a lawyer

Rest of the World

Country	Law	IP Address personal data	Consent based	Extraterritorial
European Union	GDPR – General Data Protection Regulation	Yes	Yes	Yes
Brazil	LGPD - Lei General de Protecao de Dados Pessoals	Yes (not explicitly stated)	Yes	Yes
China	PIPL - Personal Information Protection Law	Yes	Yes	Yes
Japan	APPI - Act of Protection of Personal Information	Yes (including anonymized data)	Yes	Yes
Canada	PIPEDA - Personal Information Protection and Electronic Documents Act	Yes	Yes (implicit)	Yes

Annex: GDPR & IETF Standards

Not that far away

Annex A: RFC 8280

Human Right Protocol Considerations

https://datatracker.ietf.org/doc/rfc8280/

Research into Human Rights Protocol Considerations – RFC 8280

- Purpose of the document:
    - document aims to propose guidelines for human rights considerations

- Why it is important?
    - It touches topics related to GDPR like:
        - Connectivity
        - Privacy
        - Security
        - Anonymity
        - Localization
        - Reliability
        - Confidentiality
        - Integrity
        - Authenticity
- Following slides cover excerpts of RFC 8280 of those parts or questions that somehow relate to GDPR and the IP layer

5.2.3.1.1. Network Visibility of Source and Destination

- **“Inclusion of an Internet-wide identified source in the IP header is not the only possible design,…”**
- **“A variety of alternative designs do exist,…**.”

- The above sentence basically state that obfuscating the IP addresses is sometimes desirable and that their presence in clear is not a technical must

- This relates to GDPR in the sense that having IP addresses in clear is not strictly necessary for an ISP to provide Internet services

Annex B: RFC 6973

Privacy Considerations for Internet Protocols

https://www.rfc-editor.org/rfc/rfc6973

Privacy Considerations for Internet Protocols – RFC 6973

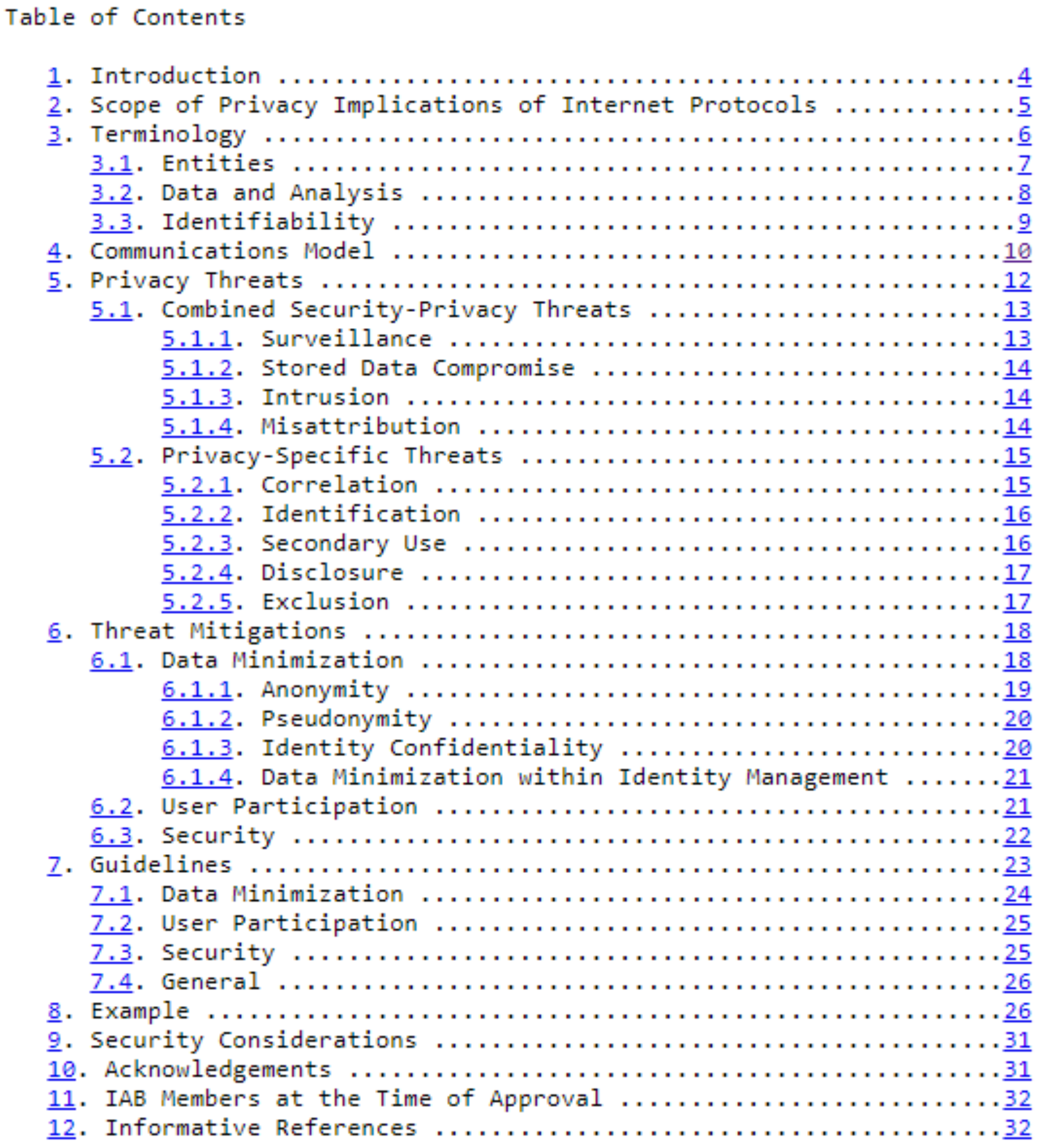


Table of Contents

- *“This document offers guidance for developing privacy considerations for inclusion in protocol specifications.”*

- The document has a broad scope including terminology, models, privacy threats
  - Interesting reading

- Relevant parts:
  - 6. Threat Mitigation
  - 7. Guidelines

Threat Mitigation (I)

- Data Minimization

> “Data minimization refers to collecting, using, disclosing, and storing the minimal data necessary to perform a task. Reducing the amount of data exchanged reduces the amount of data that can be misused or leaked.”

  - Like GDPR this document suggest to reduce data to a minima just to perform the task at hand
    - E.g. IP packets forwarding does not need access to higher layers’ headers or payload

- Anonymity

> “.... anonymity is relative with respect to the observer or attacker.”

  - E.g. my access network may need to know who I am because of access rights (think about a VPN) but beyond the local access there is no need to know who I am in order to forward packets (beyond the VPN)

Threat Mitigation (II)

- Pseudonimity

> "For Internet protocols, the following are important considerations: whether protocols allow pseudonyms to be changed without human interaction, the default length of pseudonym lifetimes, to whom pseudonyms are exposed, how individuals are able to control disclosure, how often pseudonyms can be changed, and the consequences of changing them."

  - E.g. if you consider IP a pseudonym then it is desirable to change them regularly in an automated way
    - Think for instance IPv6 temporary addresses (RFC 4941)

- Security goals
  - o Confidentiality: Keeping data secret from unintended listeners. <= Principle 6 GDPR: SECURITY (INTEGRITY AND CONFIDENTIALITY)
  - o Peer entity authentication: Ensuring that the endpoint of a communication is the one that is intended. <= No counterpart in GDPR
  - o Unauthorized usage: Limiting data access to only those users who are authorized. <= Principle 7 GDPR: ACCOUNTABILITY
  - o Inappropriate usage: Limiting how authorized users can use data. <= Principle 1 GDPR: LAWFULNESS, FAIRNESS AND TRANSPARENCY

Relevant Guidelines (II)

- RFC 6973 does as well provide guidelines for user control
  - However, user does not have direct control over the Network level and the only “control” that it has is whether or not to accept the Service Level Agreement
  - Yet, the question may be asked whether or not a user can ask to delete all information regarding the IP address that he/she used throughout all ASes? GDPR provide the “right to be forgotten”, can my IP address be forgotten?

- Another general point is:

> “a. Trade-offs. Does the protocol make trade-offs between privacy
> and usability, privacy and efficiency, privacy and
> implementability, or privacy and other design goals? Describe
> the trade-offs and the rationale for the design chosen.”

  - <u>There is always an engineering trade-off to be made between privacy, usability, implementability</u>

Thank you!

Questions?