EU Going Dark HLG
Nye tiltag mod kryptering?

Jesper Lund
IT-Politisk Forening
jesper@itpol.dk

Cryptohagen
25. august 2024

Hvad er Going Dark HLG

- **Ikke konkret lovforlag** som Chat Control
- HLG er en arbejdsgruppe (ekspertgruppe)
  - Anbefalinger fra HLG maj 2024
  - Input til næste Kommission, ikke officiel politik p.t.
- Fokus på at fremme ”adgang til data” for politiet
  - Udfordringer skabt af kryptering
  - Manglende tilgængelighed for data (logning)

HLG hjemmeside

9 JULY 2024

High-Level Group (HLG) on access to data for effective law enforcement

PAGE CONTENTS

The **High-Level Group (HLG) on access to data for effective law enforcement**, launched by the Commission in June 2023, and co-chaired by the Commission and the rotating Presidency of the Council of the EU explores any challenges that law enforcement practitioners in the Union face in their daily work in connection to access to data and potential solutions to overcome them, with the aim of ensuring the availability of effective law enforcement tools to fight crime and enhance public security in the digital age, in full respect of fundamental rights.

Mission

The objectives of the HLG are to:

- Establish a **collaborative and inclusive platform for stakeholders** from all relevant sectors, including law enforcement, data protection experts, private sector operators, NGOs, and academia, to work towards commonly accepted solutions.
- Formulate a **strategic forward-looking vision** on how to address current and anticipated challenges against the background of technological developments, enabling a comprehensive EU approach to ensure access to data for effective law enforcement.
- Propose **recommendations** for the further **development of Union policies** to enhance and improve access to data for the purpose of effective law enforcement.

Kritik af HLG

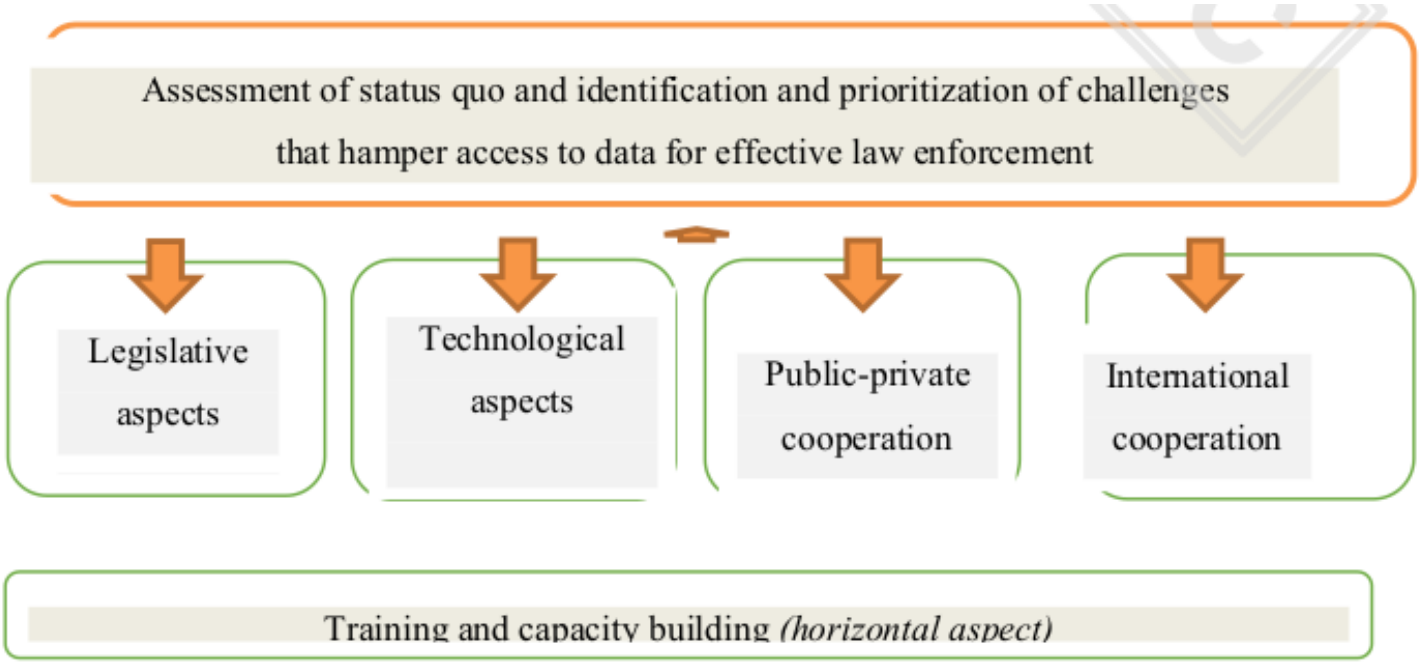
- Anti-kryptering tilgang
  - Berettiget frygt for kommende lovforslag med krav om bagdøre ala Chat Control
- Ingen transparens og demokratisk legitimitet
  - HLG fordi der for High-Level **Expert** Groups (HLEG) er krav om transparens og repræsentation
- Ingen ny indsigt eller løsningsforslag fra HLG

Det uløselige problem (30+ år)

- Anbefaling nr. 26 (TL;DR nedsæt ny HLG..)
  - **Establishing a research group to assess the technical feasibility of built-in lawful access obligations** (including for accessing encrypted data) for digital devices, while maintaining and without compromising the security of devices and the privacy of information for all users as well as **without weakening or undermining the security of communications.**

EDRi: mission failure

Planen for HLG (april 2023)



HLG scoping paper (1/2)

- Bagdør i ny forklædning (fra 8281/23)
  - The HLEG **will demonstrate** that security can be effectively strengthened whilst being in full compliance with the highest data protection and justice standards and safeguards. The concept of ‘security by design’ i.e., **combining access by design and privacy by design** is important in this context and will be explored to the full.

HLG scoping paper (2/2)

- Grundlæggende rettigheder?
  - The HLEG will address the issue from the perspective of the victims of crime **and the protection of potential victims**.
- Bagdøre via tekniske standarder
  - Participation of law enforcement representatives in relevant international standardisation bodies **such as [..] 3GPP**
  - Ikke ny idé - i 2020 havde de også kig på IETF standarder på internettet (fx TLS)

HLG arbejdsgrupper

- **WG 1:** Access to data at rest in a user's device
  - On-device kryptering (fysisk adgang)
- **WG 2:** Access to data at rest in a provider's system
  - Logning og e-evidence
- **WG 3:** Real-time access to data in transit
  - Aflytning af E2EE kommunikation

HLG deltagere

- Kommissionen (især DG HOME)
- EU-regeringerne
- Europol, Eurojust, EU CTC, m.v.
- EDPS og EDPB (observatørstatus)
- Inviterede eksperter
  - Academia, standard organisationer og virksomheder
  - Ingen NGO’er (anmodning blev afvist)

NGO anmodning om at bidrage

Dear co-Chairs of the High-Level Group,

I am writing on behalf of IT-Political Association (IT-Pol) which promotes and defends digital rights in Denmark and is a member of European Digital Rights (EDRi).

We would like to put ourselves forward as civil society experts and participants to the upcoming activities and working sessions of the High-Level Group (HLG) on access to data for effective law enforcement that are pertaining to our mission.

As an NGO working in the field of data protection and privacy for more than 10 years, we are able to contribute with specific expertise to the overall objectives of the HLG. Specifically, IT-Pol has worked on data retention at the national (Danish) and EU level, on the e-Evidence Regulation and the Second Additional Protocol to the Budapest Convention in cooperation with EDRi, and on policy issues related to encryption (likewise together with EDRi). This work includes consultation responses, expert testimony to the Danish Parliament, policy and legal analysis in EDRi-gram (a publication of EDRi), as well as active contribution to a number EDRi position papers and EU-level consultation responses in these areas. Online links to samples of this work can be provided upon request.

Given our expertise and long-term engagement with these topics, we believe that we can support the HLG in assessing the interaction between the various fundamental rights at play that set up the safeguard framework for law enforcement access to data as well as the technological challenges at stake.

We are committed to helping the HLG to propose solutions in full compliance with fundamental rights at the end of its mandate.

HLG svar: go away..

Dear Jesper Lund,

Thank you for your email.

We appreciate your interest in contributing to the upcoming activities of the High-Level Group (HLG) on access to data for effective law enforcement.

The HLG welcomes written contributions on specific topics under discussion within its Working Groups, namely:
1) access to data at rest in a user's device;
2) access to data at rest in a provider's system; and
3) access to data in transit ('real time access').

Such contributions should be sent to EC-HLG-GOING-DARK@ec.europa.eu.

Please note that, by submitting your written comments, you acknowledge that your contribution might be shared with the members of the Working Groups. It is also important to note that your contribution may be subject to a request for access to documents under Regulation 1049/2001 on public access to European Parliament, Council, and Commission documents. In this case, the request will be assessed against the conditions set out in the Regulation and in accordance with applicable data protection rules.

Should your contribution prove pertinent to the on-going discussions, the co-chairs of the HLG might extend an invitation for you to present your views in one of the Working Groups via WebEx.

Mørklægning (aktindsigt)

List of Participants of the 1st Meeting of Working Group 3

(Real time access to data in transit)

4 October 2023

FIRST NAME	SECOND NAME	NATIONALITY / INSTITUTION
[redacted]	[redacted]	BE
[redacted]	[redacted]	CZ
[redacted]	[redacted]	DE
[redacted]	[redacted]	DE
[redacted]	[redacted]	EL
[redacted]	[redacted]	ES

WG-1 highlights

- Access-proof devices (ingen dokumentation)
- Forensics tools (fx Cellebrite) er dyre og udvikles ofte uden for EU
- Vidensdeling blandt EU-lande (national sikkerhed!)
- Ønske: samarbejde med hardware producenter
  - Sustained, long-term engagement with standardisation bodies **to ensure that lawful access protocols are built into devices and applications before they enter the market.**

WG-3 highlights (1/2)

- Level playing field mellem OTT udbydere og telecoms
- Magical thinking om E2EE tjenester
  - Outlining an approach to address **through standards** the development of communication technologies that would enable lawful access **without weakening cybersecurity mechanisms.**
  - When ensuring the possibility of lawful access by design as provided by law, manufacturers or **service providers should do so in a way that it has no negative impact** on the security posture of their hardware or software architectures.

WG-3 highlights (2/2)

- Samarbejde med udbydere
  - Microsoft referred to the technical work already conducted to develop lawful interception in real time capabilities of for Skype calls or Teams services.
- **Sanktioner mod udbydere**, der ikke vil samarbejde (ikke kun tjenester som EncroChat)
- Blokering af ”non-compliant” udbydere

Offentlig høring

- Efter klager over lukket proces kom der en invitation til offentlig høring 20. februar 2024
- Mange deltagere (130+), **men ikke reel høring**
  - Ingen oplæg fra HLG om deres arbejde
  - EDRi m.fl. kunne give input til de tre WG områder
- EDRi skriftligt høringssvar

Vores protester virker!

- HLG ser den offentlige debat som et problem
  - Furthermore, the **current state of the public discourse** concerning privacy and security, which are at times erroneously contrasted, was proposed as a factor which **might have negatively affected the development of legislation to develop lawful pathways** for law enforcement authorities to access data.
- **Warning!!** HLG strategi om at omdefinere begreber, fx ”security by design” og hvad der (ikke) er en bagdør

Hvad sker der så nu..?

- HLG anbefalinger til den nye Kommission
- Forslag om aflytning af E2EE tjenester?
  - **Ja:** Konsensus om at få denne mulighed
  - **Nej:** ingen aner hvordan det skal gøres uden at svække sikkerheden (og det vil man ikke, officielt)
  - Måske en ”Chat Control” model, hvor tjeneste-udbyderne får ansvaret for at **gøre det umulige**?