France's Recent Proposals for DNS Blocking in Browsers

Mallory Knodel, CDT

(proposed) Military Planning Law (LPM) 2024–2030

1. Text (French): https://www.assemblee-nationale.fr/dyn/16/textes/l16b1033_projet-loi#D_Chapitre_V_39
2. This bill sets military planning strategy for 2024-2030. The bill was just passed by France's lower house. Passed French Senate. Now text needs to be harmonized between two houses and implemented.
    a. Under the rationale of protecting the French Republic from debilitating cyber attacks, and using "modern techniques" it gives National Information Systems Security Authority (ANSSI) authority to:
        i. Require DNS providers (including resolvers) to block domains without a court order
        ii. Require software vendors to disclose vulnerabilities whether or not they've been patched
        iii. Require communications providers to disclose non-identifying internet traffic upon request
        iv. Install data collection tools in data centers without a court order.
    b. Many civil liberties complaints at a high level: https://www.pbs.org/newshour/world/lawmakers-approve-bill-allowing-french-police-to-locate-suspects-by-tapping-their-devices

(Proposed) Digital Bill

1. Link (French): https://www.legifrance.gouv.fr/dossierlegislatif/JORFDOLE000047533100
2. This is a separate bill on digital policy that is ostensibly aimed at transposing the Digital Services Act, the Digital Markets Act, and EU Data Governance Act, but goes far beyond in a number of key areas. The draft bill has been reviewed by the Senate. Next stop goes to the National Assembly in September.
    a. It contains similar provisions to the military planning law:
        i. Require DNS providers (including resolvers) to block domains without a court order
        ii. Require browsers to block domains without a court order and serve users warnings
    b. Media freedom, age verification and other human rights concerns: https://www.euractiv.com/section/platforms/news/france-mulls-new-frontline-digital-bill-going-beyond-eu-rules/?_ga=2.89111067.1270439537.1688376930-1669050714.1683052757

Response

“... Individuals in our personal capacities who have devoted their careers and lives to building a safer, more reliable, and more inclusive Internet…”

- Vinton G. Cerf, Internet Pioneer and Former Chairman of ICANN
- Stephen D. Crocker, Internet Pioneer and Former Chairman of ICANN
- Mirja Kühlewind, Internet Architecture Board Chair
- Mallory Knodel, Internet Architecture Board Member and Chief Technologist at the Center for Democracy and Technology
- Carl E. Landwehr, University of Michigan
- Wes Hardaker, Internet Architecture Board Member and Senior Computer Scientist at the University of Southern California’s Information Sciences Institute
- David Schinazi, Polytechnicien and Internet Architecture Board Member
- Joseph Lorenzo Hall, PhD, Distinguished Technologist, Internet Society
- Suresh Krishnan, Internet Architecture Board Member
- Erik Kline, IETF Internet Area Director
- Alexis Hancock, Electronic Frontier Foundation
- Wendy Seltzer, Principal Identity Architect, Tucows

Arguments

1. Ineffective: “We are deeply concerned that these measures will do little to address the underlying cyber risks our societies face…”
2. Overreach: “… while inadvertently creating or exacerbating other sources of risk.”
3. **Global impacts on internet and internet governance**: “... might set a troubling precedent that could inspire similar measures in democratic and non-democratic jurisdictions alike — with global implications for security and online freedom.”

Impacts on the internet

1. Impacts to the Domain Name System
    a. DNS blocking
    b. Shutdowns via DNS
    c. Non-ISP DNS resolvers no matter jurisdiction must also comply
    d. Proposed alternatives: Blocking HTTP/HTTPS connections to the offending site, blocking site IP addresses, seizing domains.
2. Impacts to Web Browsing
    a. Browsers must block access to problematic websites and flag to users.
    b. Proposed alternative: Use Safe Browsing and existing mechanisms.

Impacts on the internet (cont)

4. Warrantless (Mass) Surveillance
    a. ANSSI can install hardware and software enabling the collection of user data on networks at data centers.
    b. Centralises response to cyber incidents.
    c. Proposed alternative: Work with established frameworks for incident response and threat intelligence.
5. (Unsafe) Premature Vulnerability Disclosure Risks
    a. Requires a vulnerability to immediately be reported to ANSSI.
    b. Proposed alternative: Do not contravene best practice which is to consider the state of vulnerability patch before disclosure.

Full letter

Sent to ‘Distinguished Members of the French Assembly and Senate’ on 23 June 2023

Available at:
https://medium.com/@vgcerf/concerns-over-dns-blocking-988ef546a100