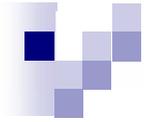




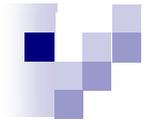
10 trends of internet censorship revisited

Päivikki Karhula, chief information
specialist
Finnish Parliament Library
Email. Paivikki.karhula@gmx.com



10 trends

- n "Free internet" is dead
- n Western democracies extend controls
- n Complexity
- n Criminalization of everyday life
- n Ubiquitous technologies extend surveillance into objects and persons
- n Database citizenship
- n Privatization of the Internet
- n Copyright as censorship
- n Intermediaries as controllers
- n Erosion of civil rights and democracy



Variety of methods

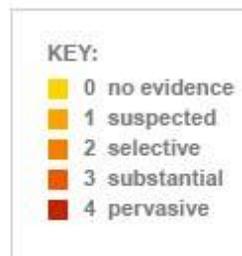
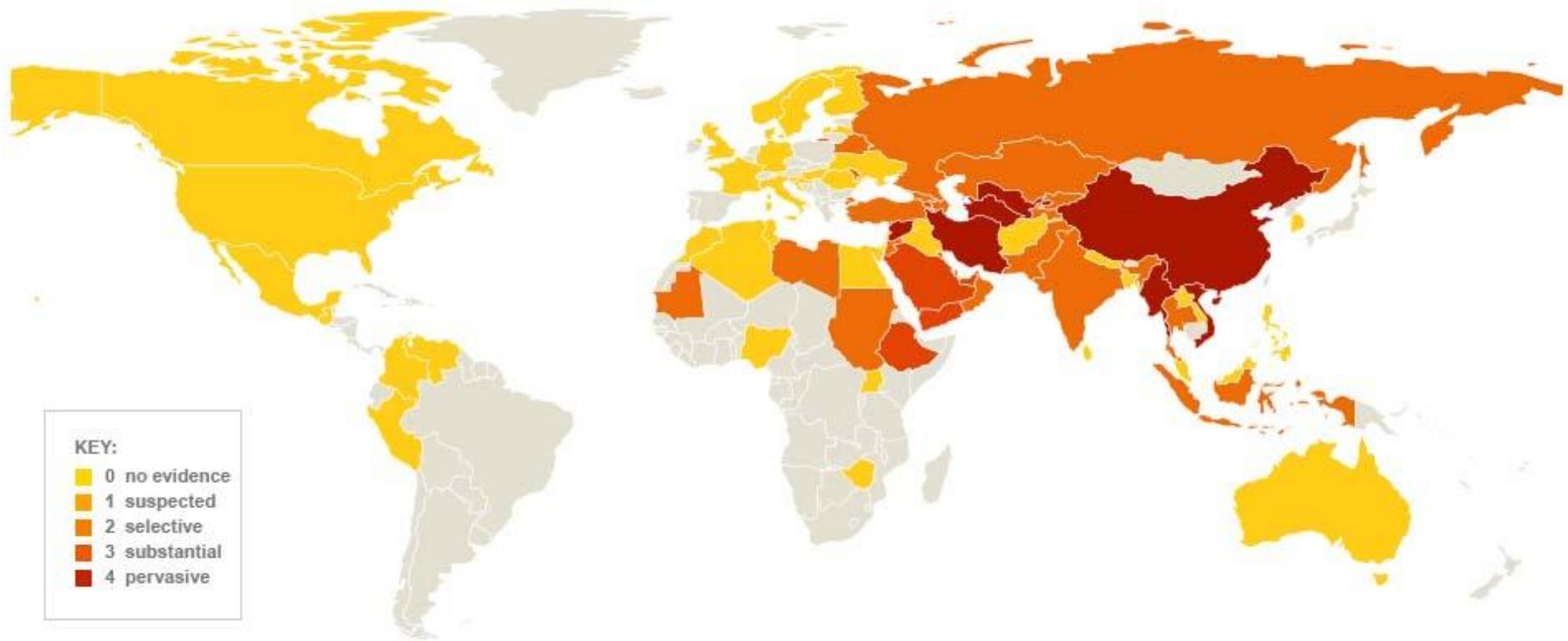
- n Identification
- n Tracking
- n Monitoring
- n Data collection
- n Data storage
- n Data analysis
- n Slowing down connections
- n Filtering
- n Blocking
- n Restricting access
- n Sanctioning



Severity varies

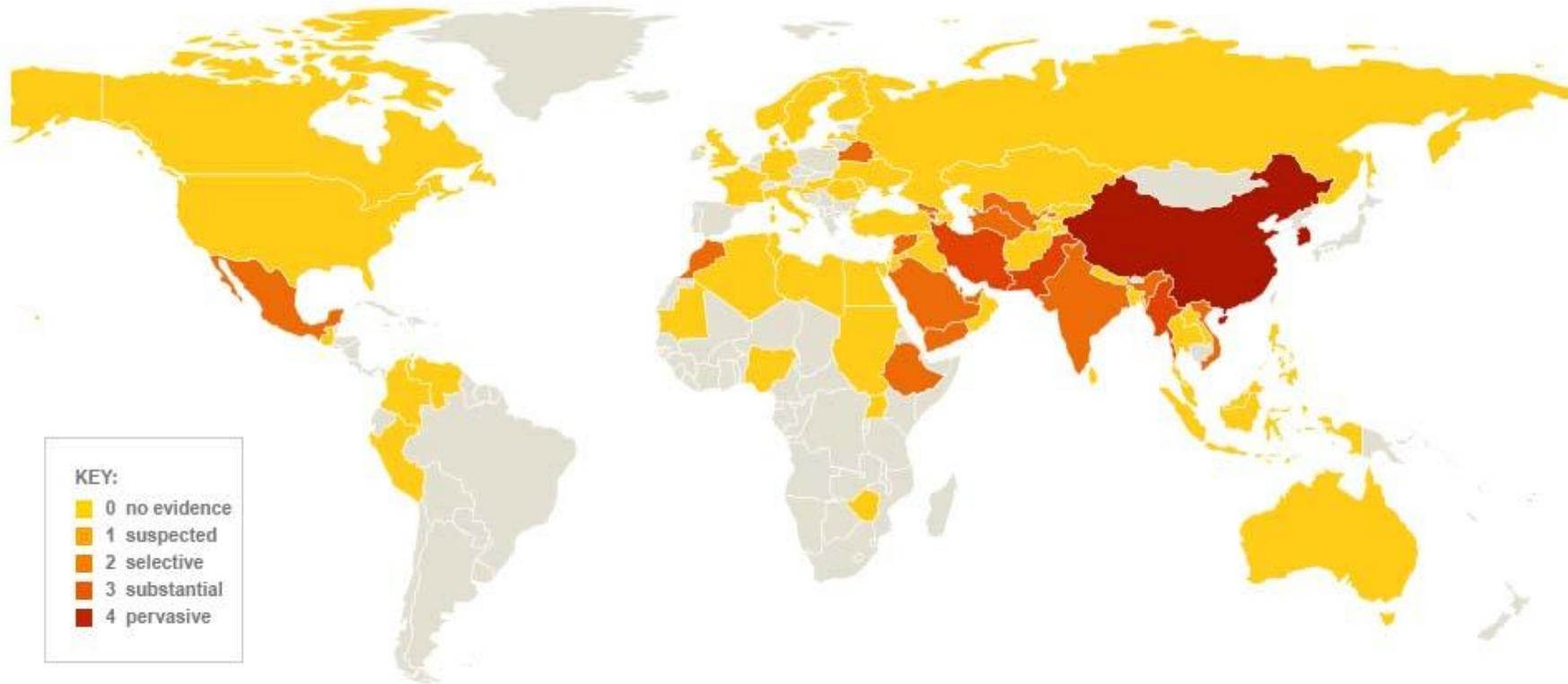
- n Pervasive
- n Substantial
- n Selective
- n Under surveillance
- n Non-existent
- n Death penalties
- n Detention, fines
- n Criminal charges
- n Interrogation, raids
- n Soft penalties

Category: **Political**



Open Net Initiative, Interactive Map of Censorship,
<http://www.theguardian.com/technology/datablog/interactive/2012/apr/16/web-filtering-censorship>

Category: **Conflict/Security**



- Political
- Social
- Tools
- Conflict/Security**
- Transparency
- Consistency

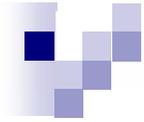
Open Net Initiative, Interactive Map of Censorship,
<http://www.theguardian.com/technology/datablog/interactive/2012/apr/16/web-filtering-censorship>



International involvement

- n International agreements & standards
- n International pressure
- n International support practices
- n *EU*
 - .. Prohibited export of surveillance technologies to totalitarian countries
 - .. Support to connectivity for activists in totalitarian countries
 - .. No asylum to whistleblower (Snowden)

Criminalization of everyday life



Libraries

- n Mass data collection
- n User recognition
- n Location tracking
- n Access control
- n E-book surveillance

E-Reader Privacy Chart, 2012 Edition

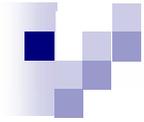
See our announcement of this chart's launch [here](#).

Can they keep track of searches for books?								
Google Books	Amazon Kindle	Barnes & Noble Nook	Kobo	Sony	OverDrive	IndieBound	Internet Archive	Adobe Content Server
Yes Logs all search data with IP address. Will also associate searches with user's Google Account if logged in. Will not associate	Yes/Unclear Logs data on products viewed and/or searched for on the device, and associates info with Amazon account. Searching the Inside Book feature requires login	Yes/Unclear The privacy policy indicates that searches made on the Nook are probably not recorded, but B&N generally logs data on searches made and pages viewed on B&N	Yes Kobo seems to have the capability to keep track of book searches because it indicates that it shares those searches with third parties.	Yes Sony seems to collect information on "site interaction," which presumably includes uses of the Reader Store, and on "network-enabled devices."	No Appears not to track searches of books on library sites.	Unclear While IndieBound's reader app seems not to have a distinct privacy policy, the site policy indicates that it collects "non-personal, aggregate information such as	No The Archive does not collect IP addresses or user-identifiable data about book searches.	No The Adobe Content Server software cannot monitor what a user reads.

<https://www.eff.org/pages/reader-privacy-chart-2012>



NSA-leak & Snowden as a game changer



Impacts

- n Immense consequences
- n Global media campaign
- n Exceptional scale of media attention
- n Raising citizens awareness
- n Political interest



“ From both an operational and a symbolic perspective there could be a major push by the US for even greater travel surveillance and data collection at a global level.

”

Third – when the smoke finally lifts - **the true information security implications of the PRISM/Snowden affair will become clear.**

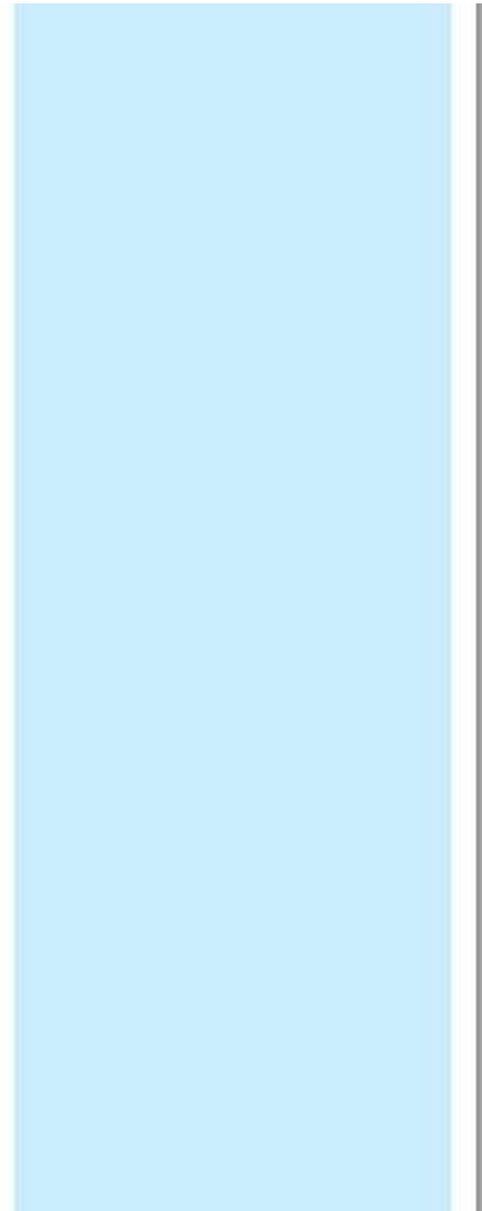
Snowden was a relatively low-level contractor. Governments and the public have yet to digest the security implications of a spying system involving many hundreds of system administrators that appears to be held together with little more than template secrecy agreements. This could possibly result in a push to eliminate external contractors and bring NSA activities "in house". This option is already being widely *discussed*.

Fourth, a pragmatic and a moral imperative has been created that may **accelerate funding and investment for research into technologies of circumvention.** This trend would in itself, however, provide the NSA with weaponry to push back against greater transparency of its activities.

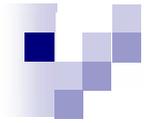
Such a response occurred in the 1990s during the "crypto wars" when the US government attempted to regulate encryption development and deployment. The proposed restrictive policy triggered a centre of gravity that attracted significant interest in circumvention.

Fifth, the revelations will continue to spark renewed interest in **strengthened privacy protections in other parts of the world.** As noted in previous *articles* on this site, hitherto successful lobbying by the US to weaken privacy protections in emerging European and Indian law may now be nullified as parliamentarians reconsider their compliant position.

Sixth, connected directly with the point above, **online providers will need to take privacy more seriously.** The first wave of the PRISM story detailed NSA access to the servers of Google Apple and other companies – a situation that the companies deny knowledge of. However as the controversy widens there will be increased focus on what steps these providers are taking to avoid becoming outsourced storage facilities for security agencies.



Simon Davies, Analysis: Eight global repercussions from the PRISM disclosures
<http://www.privacysurgeon.org/blog/incision/analysis-eight-global-repercussions-from-the-snowden-affair/>



Impacts

- n Alternative services and technologies
- n Business impact
- n Interest in development of innovations and technologies to privacy protection
 - .. E.g. localizing of cloud services



Raised questions



Power transfer

n Power transfer

- .. Data ownership, data management

n Consequences

- .. How this data is used?

n Unlimited scope

- .. Unlimited data collection, unlimited authorities

n Non-transparency

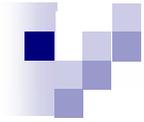
- .. Secret institutions, secret principles, secret practices, secret interests



Governance

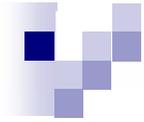
n Democratic principles, rules of good governance

- .. Transparency
- .. Accountability
- .. Participation
- .. Legitimacy of actions...



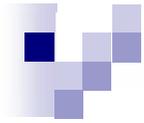
Future extensions

- n New forms of surveillance
 - .. User recognition
 - .. Locating
 - .. Extended data collection...



Protections

- n What kind of protections exists against excessive surveillance?
- n What kind of new protections would need to be developed?
- n NGOs activated



Libraries

Freedom of information =

Access to internet

+

Safe access to communicate, search and
use information on internet

+

Democratic structures



What to do...

n Involve in development of...

- .. Marketplace
- .. Technologies
- .. Policies & practices
- .. Legislation

“Globally, we are seeing increasing debate –amongst both state and non-state actors – about whether or not and how to regulate freedom of expression online. **In the next two to three years, these debates are likely to lead to crucial decisions including whether or not to establish top-down control of the internet** – something EU member states and the US currently oppose in favour of a more diverse and bottom-up multistakeholder approach. With China and Russia pushing for greater government control, these debates are acquiring a strong geopolitical dimension.”

Index on Censorship Policy paper, 20.6.2013

<http://www.indexoncensorship.org/2013/06/is-the-eu-heading-in-the-right-direction-on-digital-freedom/>

Case: Lex Snowden. Finnish Citizens' legislative initiative against citizens surveillance and whistleblower protection.

<http://vimeo.com/72412202>

MARCH 31, 2011 | BY KATITZA RODRIGUEZ



EFF to Council of Europe: Ensure Privacy, Transparency, and Freedom of Expression in Search Engines

This week the Council of Europe's [expert committee on new media](#) (MC-NM) met in Strasbourg to examine the comments received on the [draft recommendation](#) and proposal for [guidelines](#) for search engines.

In [written comments](#), EFF urged the Council of Europe to revise its recommendation and guidelines to ensure that they promote transparency on search records requests, protect privacy vis-à-vis the government, and preserve freedom of expression rights, including readers' rights to read information online. EFF also commented favorably on language that acknowledges that search engines play a central role as intermediaries by enabling the public to seek, impart and receive information and ideas worldwide.

Because search engines play a central role as intermediaries, search engine records contain sensitive information about a person's intellectual, political, cultural, religious, psychological, and physical (health) beliefs, conditions and actions that can be of interest to state actors and civil litigants. These search records pose the most obvious privacy threat, since they represent some of the most sensitive data about individuals. Other potential threats to personal data come in the form of subpoenas, unauthorized access, civil litigants' requests, computer hackers, and compelled disclosure of search records to law enforcement and national security investigators.

Donate to EFF



Stay in Touch

Email Address

Postal Code (optional)

SIGN UP NOW

NSA Spying



eff.org/nsa-spying

EFF is leading the fight against the NSA's illegal mass surveillance program. [Learn more](#) about what the program is, how it works and what you can do.

Follow EFF

<https://www.eff.org/deeplinks/2011/03/eff-council-europe-ensure-privacy-transparency-freedom-expression>



What to do...

- n Co-operation, advocacy
 - .. Statements
 - .. Campaigns
 - .. Focus
 - n Issues
 - n Scope (international, national, local)



Possible partners

n IFLA / FAIFE

n Library associations

n Libraries

n NGOs

.. EFF

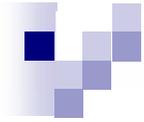
.. ONI

.. Freedom house

.. Privacy international

.. Reporters without
borders

.. Transparency
international



What to do...

n Learn & teach

- data and privacy protection practices



Browse Privacy Topics

[Privacy Basics](#)

[Background Checks & Workplace](#)

[Banking & Finance](#)

[Credit & Credit Reports](#)

[Debt Collection](#)

[Education](#)

[Harassment & Stalking](#)

[Identity Theft & Data Breaches](#)

[Insurance](#)

[Junk Mail/Faxes/Email](#)

[Medical Privacy](#)

[Online Privacy & Technology](#)

[Privacy When You Shop](#)

Fact Sheet 18: Online Privacy: Using the Internet Safely

Send to Printer

Copyright © 1995 - 2013
Privacy Rights Clearinghouse
Posted July 1995
Revised July 2013

Introduction

1. Which Online Activities Reveal My Personal Information?
 - Signing up for Internet service
 - Browsing the Internet
 - Search Engines
 - Cookies
 - Flash cookies
 - Fingerprinting
 - Householding
 - Using Mobile Apps
 - Using e-mail
 - Instant messaging

Stay Informed
join our mailing list

California Medical Privacy

Donate



Print This Page

Send to Printer

Follow Us!

Like us on Facebook!

Follow us on Twitter!

Subscribe to RSS!

Online privacy. Using the Internet Safely / Privacy Rights Clearinghouse.
<https://www.privacyrights.org/fs/fs18-cyb.htm>



ONLINE SURVIVAL KIT

This **Online Survival Kit** offers practical tools, advice and techniques that teach you how to circumvent censorship and to secure yo communications and data. This handbook will gradually be unveiled over the coming months in order to provide everyone with the means to resist censors, governments or interests groups that want to courtrol news and information and gag dissenting voices.

FIFTEEN MINUTES OF ONLINE ANONYMITY

Making sure that your communications and data are confidential is not easy. Many encryption tools are available but it can take ages to learn how to use them, to learn how to avoid leaving clues or tracks that will allow others to intercept a message or identify who sent it. So that you don't have to spend the next three years training to become a security expert, **Jean-Marc Manach**, a journalist specialized in digital privacy and security, has an interesting alternative – how to have 15 minutes of online anonymity.

[MORE](#)

A PRACTICAL GUIDE TO PROTECTING YOUR IDENTITY AND SECURITY WHEN USING MOBILE PHONES

Many activists have been tracked via their mobile phones, and some countries conduct surveillance more extensively than others. You need to assess the risk for your own activities given the practices used in your country, how high-profile your work is, and what others in your community have experienced.

[MORE](#)

LANGUAGES

العربية

中文

ENGLISH

FRANÇAIS

فارسی

РУССКИЙ

FREEDOM BAROMETER

162 NETIZENS IN
JAIL**15** NETIZENS
KILLED

We Fight Censorship / Reporters Without Borders -project.
<https://www.wefightcensorship.org/online-survival-kithtml.html>

Libraries as a safe haven