Soukromí a bezpečnost v kyberprostoru

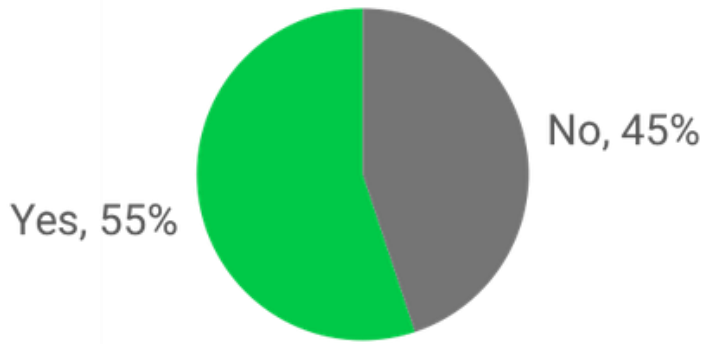
Každodennost v kyberprostoru

Kdo to je?

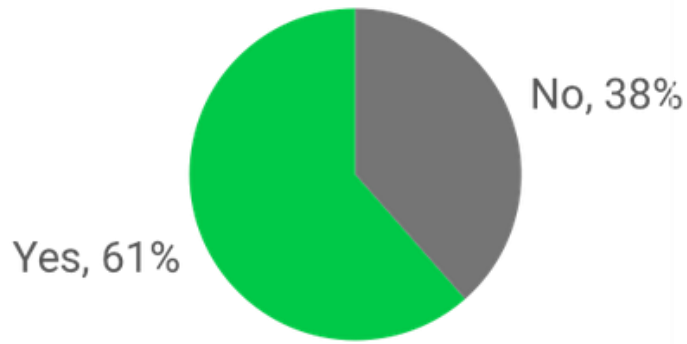
Tomáš Marek
KISK FF MUNI
marek@kisk.cz
www.marektomas.cz

Jste v anonymním režimu

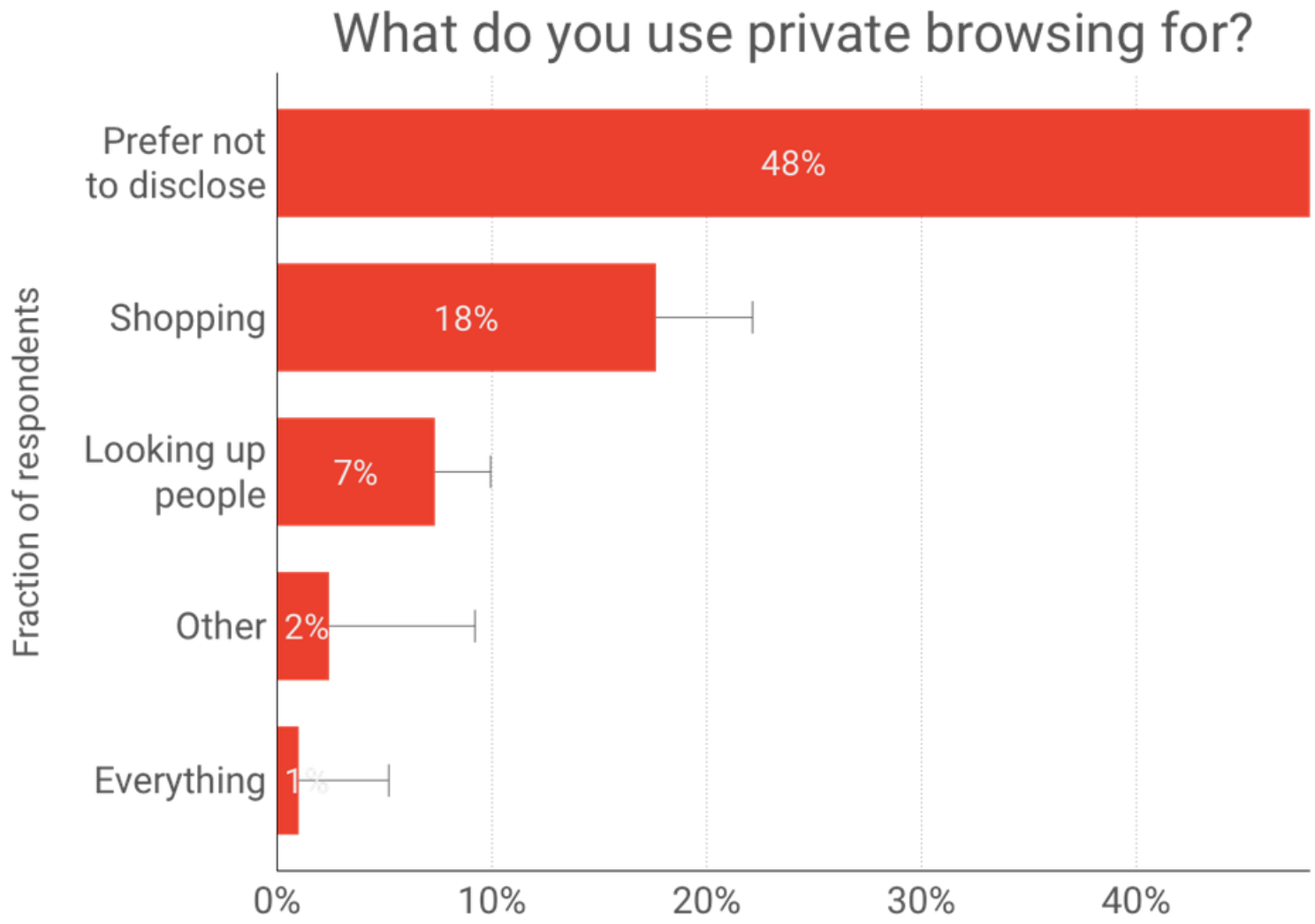
Do you know what private browsing is?

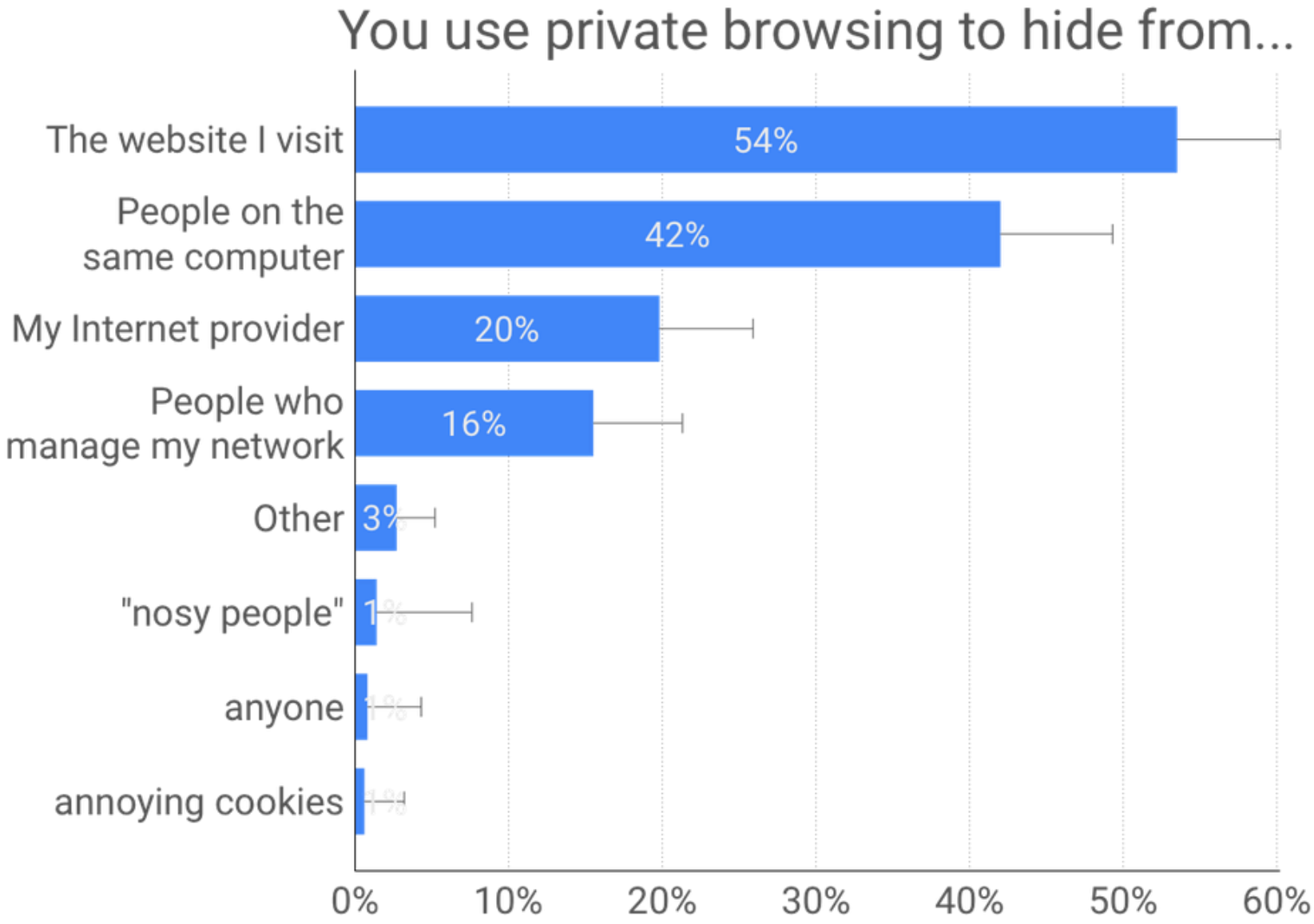


2012



2017


What do you use private browsing for?
Fraction of respondents
Prefer not to disclose
48%
Shopping
18%
Looking up people
7%
Other
2%
Everything
1%
0%
10%
20%
30%
40%


You use private browsing to hide from...
The website I visit
54%
People on the same computer
42%
My Internet provider
20%
People who manage my network
16%
Other
3%
"nosy people"
1%
anyone
1%
annoying cookies
1%
0%
10%
20%
30%
40%
50%
60%

Svoboda soukromého prohlížení na jedno klepnutí

Žádné uložené cookies ani historie, přímo z vaší plochy. Prohlížejte, jako když se nikdo nedívá.

Připnout na lištu


WHICH WEBSITE WOULD YOU LIKE TO SEE?
I DON'T WANT YOU TO KNOW
WHAT ABOUT TELLING MR. INCOGNITO?
OKAY!
@SKELETON_CLAW
SKELETONCLAW.COM

INCOGNITO BUT NOT VERY PRIVATE —

Chrome updates Incognito warning to admit Google tracks users in “private” mode

Warning added to Chrome Canary as Google settles Incognito class-action suit.

JON BRODKIN - 1/16/2024, 8:58 PM

mages | Anadolu

Jste v anonymním režimu

Jste v anonymním režimu

Ostatní uživatelé tohoto zařízení neuvidí vaši aktivitu, takže při procházení budete mít větší soukromí. Weby, které navštívíte, a služby, které použijete (včetně Googlu), budou data shromažďovat stále stejně. Stažené soubory, záložky a položky na seznamu četby budou uloženy. Další informace

Chrome nebude ukládat:

- vaši historii prohlížení,
- soubory cookie a data webů,
- údaje zadané do formulářů.

Vaše aktivita může být nadále viditelná pro následující subjekty:

- navštívené weby,
- váš zaměstnavatel nebo škola,
- váš poskytovatel internetových služeb.

Blokovat soubory cookie třetích stran

Když je tato možnost zapnutá, weby vás na internetu nemohou sledovat pomocí souborů cookie. Některé weby mohou přestat fungovat.

from Amazon for replacement blades

I happened to be on Facebook at

and starts scrolling through my Insta

ads a few days before I get

One day was talking with my friends

just pictures.

is Hammermill Color Copy 28lb,

idea of getting therapy.

for pregnancy tests and dating sit

Měli jste někdy pocit, že jste na Internetu sledováni?

„Když nemáš co skrývat…“

„Když nemáš co skrývat…“

- Jeremy Bentham - *Panopticon*
- vězení mysli
- *disident či novinář = špatný člověk?*
- společenské změny *(ponožky v sandálech?)*

„Soukromí už není sociální norma…“

„Nelze se tomu vyhnout, tak nemá cenu to řešit…“

Michal Kosinski:

- soukromí je mrtvé
- *máme tedy používat technologie?*
- řešení je odstraňování tabu, ne návrat soukromí

„Facebook’s “People You May Know” tool was outing sex workers’ real identities to their clients, and vice versa. […] A sex worker using the pseudonym Leila told me she had gone to great lengths to hide her identity from clients by using an alternate name, alternate email address, and burner phone number—contact information she didn’t provide to Facebook—yet Facebook was still inextricably linking her with her clients, suggesting them to her real-name account as people she might want to friend. “

FACEBOOK

How Facebook Schemed Against Its Users

Kashmir Hill
12/12/18 10:15AM • Filed to: ENOUGH OF THIS BULLSHIT

105 8

Photo: Getty

Last year, I was trying to solve a mystery. Facebook’s “People You May Know” tool was outing sex workers’ real identities to their clients, and vice versa, and I was trying to figure out how. A sex worker using the pseudonym Leila told me she had gone to great lengths to hide her identity from clients by using an alternate name, alternate email address, and burner phone number—contact information she *didn’t* provide to Facebook—yet Facebook was still inextricably

„Nepoužívám to, tak to nemusím řešit…“

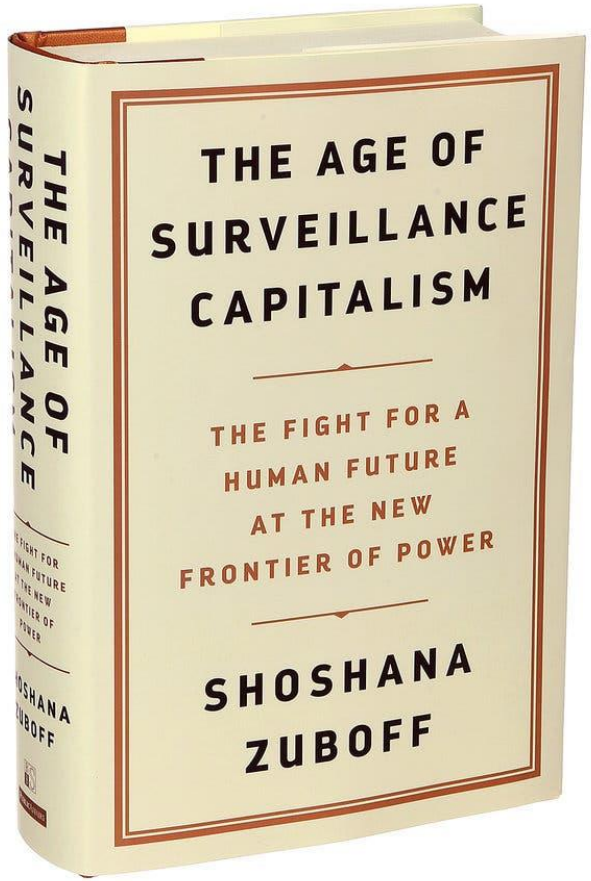
„Nepíšu nikam, co nechci, aby se vědělo.“

- metadata jsou cenná
- stínové profily
- *shadow contact*
- děti na síti – *vývoj charakteru člověka*

„Personalizovaná reklama je OK…“

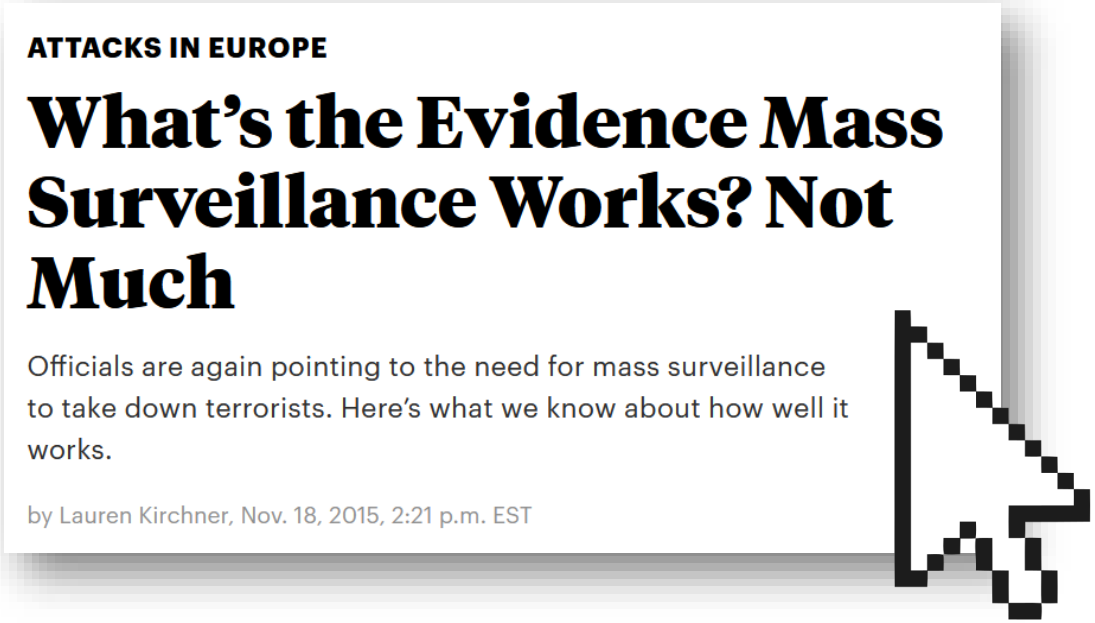
„Nějak se ty služby platit musí.“

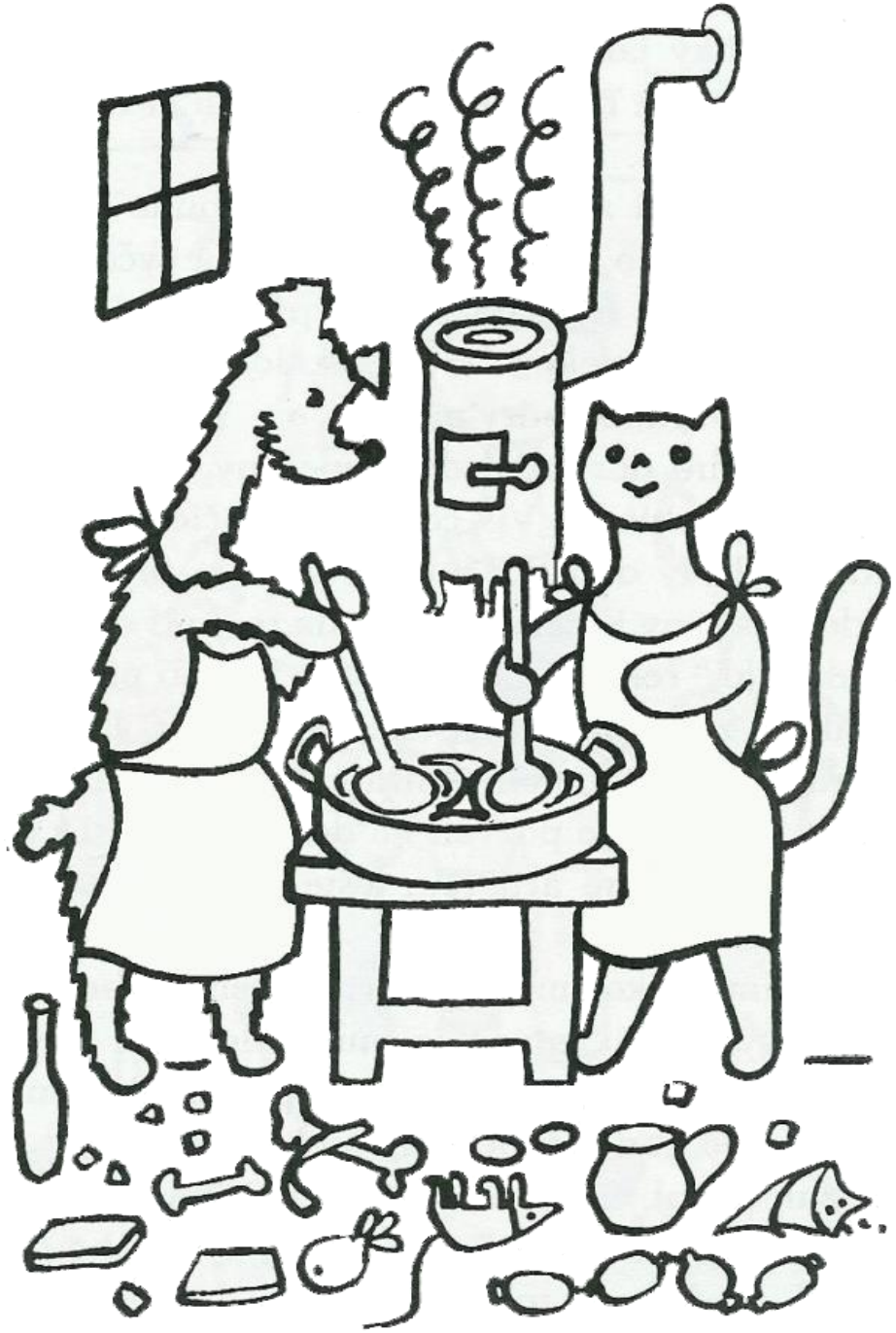
- *kapitalismus dohledu*
- Cambridge Analytica
- technologie není apolitická



„Když to pomůže zastavit špatné lidi...“

- soukromí vs. bezpečnost
- evaluace efektivity





Kdo všechno může
mít zájem nás
sledovat on-line
a proč?

Anonymita na internetu a Dark We

Anonymity is the internet's nex

https://www.theguardian.com/media-network/2015/jun/22/anonymity-internet-battleground-data-advert

Media & Tech Network

Anonymity is the internet's next big battleground

Users are growing twitchy about how their data is being used, with major ramifications for advertisers, marketers and the entire internet industry

Jon Card

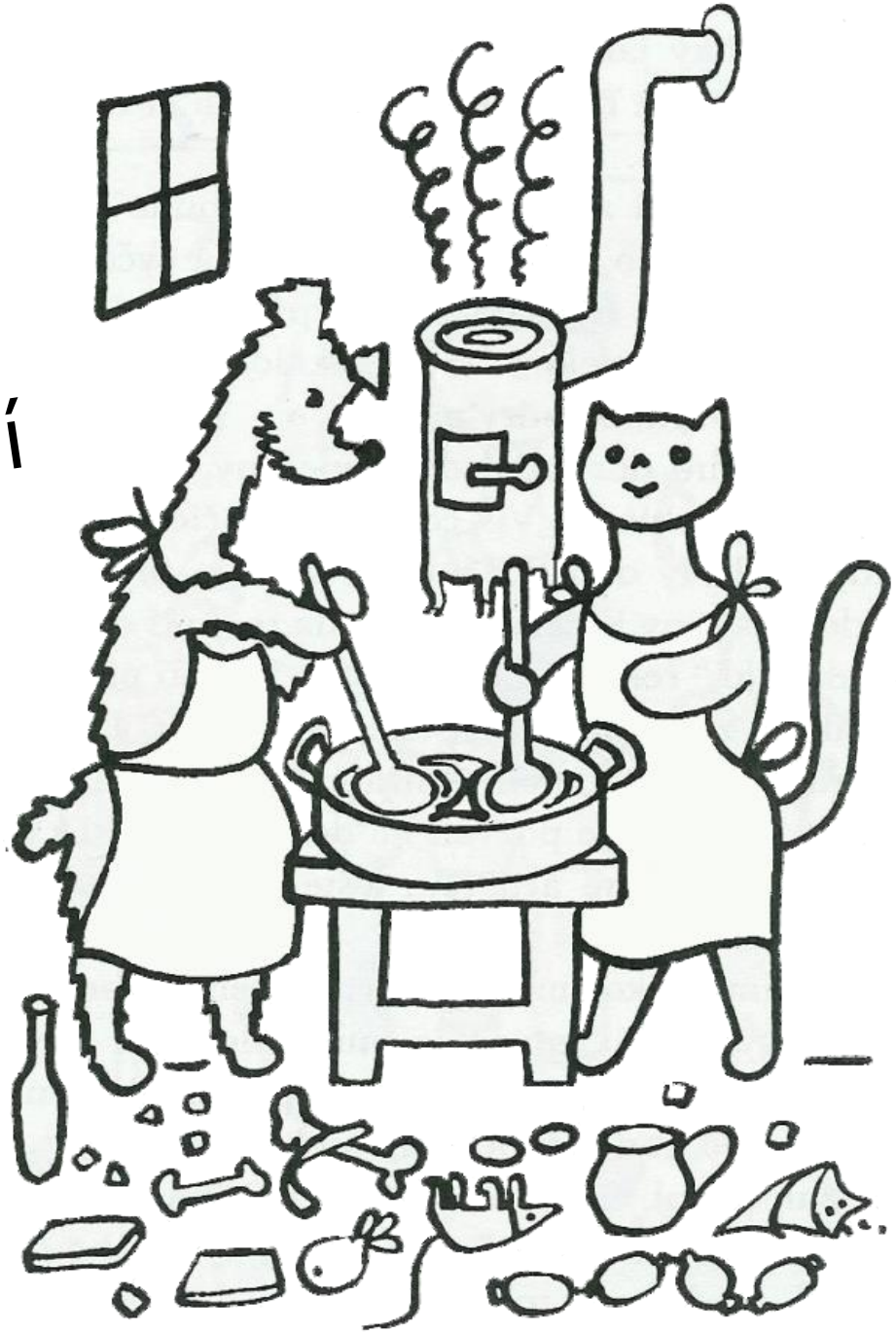
Mon 22 Jun 2015 12.00 BST

45 0

▲ Online users are rebelling against those tracking and snooping them by adopting a variety of privacy tools. Photograph: Epoxydude/Corbis

The use of personal data is a thorny subject for the public and for the many companies that use it. By allowing companies to take their data, internet users are enabling the creation of a fast, free and relevant online experience.

profilování



targeting

Michal Kosinski

modelování vlastností

od skupin k jednotlivcům

first monday
PEER-REVIEWED JOURNAL ON THE INTERNET

About ▾ Search Current Archives Announcements Submissions

Home / Archives / Volume 14, Number 10 - 5 October 2009 / Articles

Gaydar: Facebook friendships expose sexual orientation

Carter Jernigan

Behram F.T. Mistree

DOI: https://doi.org/10.5210/fm.v14i10.2611

Abstract

Public information about one's coworkers, friends, family, and acquaintances, as well as one's associations with them, implicitly reveals private information. Social-networking websites, e-mail, instant messaging, telephone, and VoIP are all technologies steeped in network data—data relating one person to another. Network data shifts the locus of information control away from individuals, as the individual's traditional and absolute discretion is replaced by that of his social-network. Our research demonstrates a method for accurately predicting the sexual orientation of Facebook users by analyzing friendship associations. After analyzing 4,080 Facebook profiles from the MIT network, we determined that the percentage of a given user's friends who self-identify as gay male is strongly correlated with the sexual orientation of that user, and we developed a logistic regression classifier with strong predictive power. Although we studied Facebook friendship ties, network data is pervasive in the broader context of computer-mediated communication, raising significant privacy issues for communication technologies to which there are no neat solutions.

HTML

Published
2009-09-25

How to Cite
Jernigan, C., & Mistree, B. F.
Facebook friendships expos
orientation. *First Monday, 14*
https://doi.org/10.5210/fm.

More Citation Formats

Issue
Volume 14, Number 10 -
2009

Section
Articles

PNAS PNAS PNAS PNAS

Psychological targeting as an effective approach to digital mass persuasion

S. C. Matz[a,1], M. Kosinski[b,2], G. Nave[c], and D. J. Stillwell[d,2]

[a]Columbia Business School, Columbia University, New York City, NY 10027; [b]Graduate School of Business, Stanford University, Stanford, CA 94305; [c]Wharton School of Business, University of Pennsylvania, Philadelphia, PA 19104; and [d]Cambridge Judge Business School, University of Cambridge, Cambridge, CB2 3EB, United Kingdom

Edited by Susan T. Fiske, Princeton University, Princeton, NJ, and approved October 17, 2017 (received for review June 17, 2017)

People are exposed to persuasive communication across many different contexts: Governments, companies, and political parties use persuasive appeals to encourage people to eat healthier, purchase a particular product, or vote for a specific candidate. Laboratory studies show that such persuasive appeals are more effective in influencing behavior when they are tailored to individuals' unique psychological characteristics. However, the investigation of large-scale psychological persuasion in the real world has been hindered by the questionnaire-based nature of psychological assessment. Recent research, however, shows that people's psychological characteristics can be accurately predicted from their digital footprints, such as their Facebook Likes or Tweets. Capitalizing on this form of psychological assessment from digital footprints, we test the effects of psychological persuasion on people's actual behavior in an ecologically valid setting. In three field experiments that reached over 3.5 million individuals with psychologically tailored advertising, we find that matching the content of persuasive appeals to individuals' psychological characteristics significantly altered their behavior as measured by clicks and purchases. Persuasive appeals that were matched to people's extraversion or openness-to-experience level resulted in up to 40% more clicks and up to 50% more purchases than their mismatching or unpersonalized counterparts. Our findings suggest that the application of psychological targeting makes it possible to influence the behavior of large groups of people by tailoring persuasive appeals to the psychological needs of the target audiences. We discuss both the potential benefits of this method for helping individuals make better decisions and the potential pitfalls related to manipulation and privacy.

persuasion | digital mass communication | psychological targeting | personality | targeted marketing

Persuasive mass communication is aimed at encouraging large groups of people to believe and act on the communicator's viewpoint. It is used by governments to encourage healthy behaviors, by marketers to acquire and retain consumers, and by political parties to mobilize the voting population. Research suggests that persuasive communication is particularly effective when tailored to people's unique psychological characteristics and motivations (1–5), an approach that we refer to as *psychological persuasion*. The proposition of this research is simple yet powerful: What convinces one person to behave in a desired way might not do so for another. For example, matching computer-

from that displayed in the laboratory (7). Consequently, it is questionable whether—and to what extent—these findings can be generalized to the application of psychological persuasion in real-world mass persuasion (see ref. 8 for initial evidence).

A likely explanation for the lack of ecologically valid research in the context of psychological persuasion is the questionnaire-based nature of psychological assessment. Whereas researchers can ask participants to complete a psychological questionnaire in the laboratory, it is unrealistic to expect millions of people to do so before sending them persuasive messages online. Recent research in the field of computational social sciences (9), however, suggests that people's psychological profiles can be accurately predicted from the digital footprints they leave with every step they take online (10). For example, people's personality profiles have been predicted from personal websites (11), blogs (12), Twitter messages (13), Facebook profiles (10, 14–16), and Instagram pictures (17). This form of *psychological assessment from digital footprints* makes it paramount to establish the extent to which behaviors of large groups of people can be influenced through the application of psychological mass persuasion—both in their own interest (e.g., by persuading them to eat healthier) and against their best interest (e.g., by persuading them to gamble). We begin this endeavor in a domain that is relatively uncontroversial from an ethical point of view: consumer products.

Significance

Building on recent advancements in the assessment of psychological traits from digital footprints, this paper demonstrates the effectiveness of psychological mass persuasion—that is, the adaptation of persuasive appeals to the psychological characteristics of large groups of individuals with the goal of influencing their behavior. On the one hand, this form of psychological mass persuasion could be used to help people make better decisions and lead healthier and happier lives. On the other hand, it could be used to covertly exploit weaknesses in their character and persuade them to take action against their own best interest, highlighting the potential need for policy interventions.

Author contributions: S.C.M. and M.K. designed research; S.C.M., M.K., and D.J.S. performed research; S.C.M. analyzed data; and S.C.M., M.K., G.N., and D.J.S. wrote the paper.

Conflict of interest statement: D.J.S. received revenue as the owner of the myPersonality Facebook application until it was discontinued in 2012. Revenue was received from dis-

chiefmartec.com April 2020

Marketing Technology Landscape

The Martech 5000

Total Solutions	8,000
Advertising & Promotion	922
Content & Experience	1,936
Social & Relationships	1,969
Commerce & Sales	1,314
Data	1,258
Management	601

Access all the data of this landscape & more at martech5000.com

2019
7,040 solutions

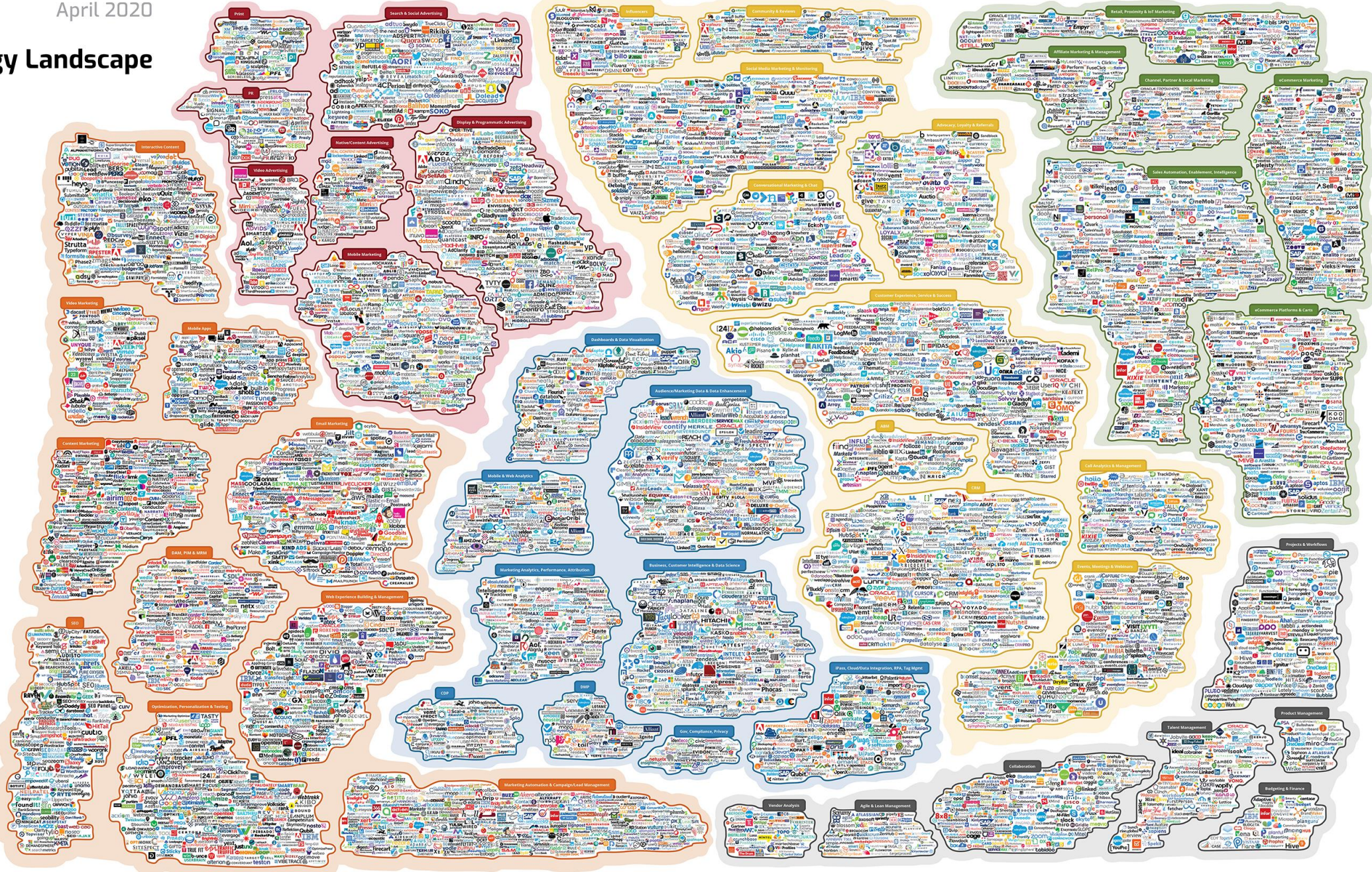
2018
6,829 solutions

2017
5,381 solutions

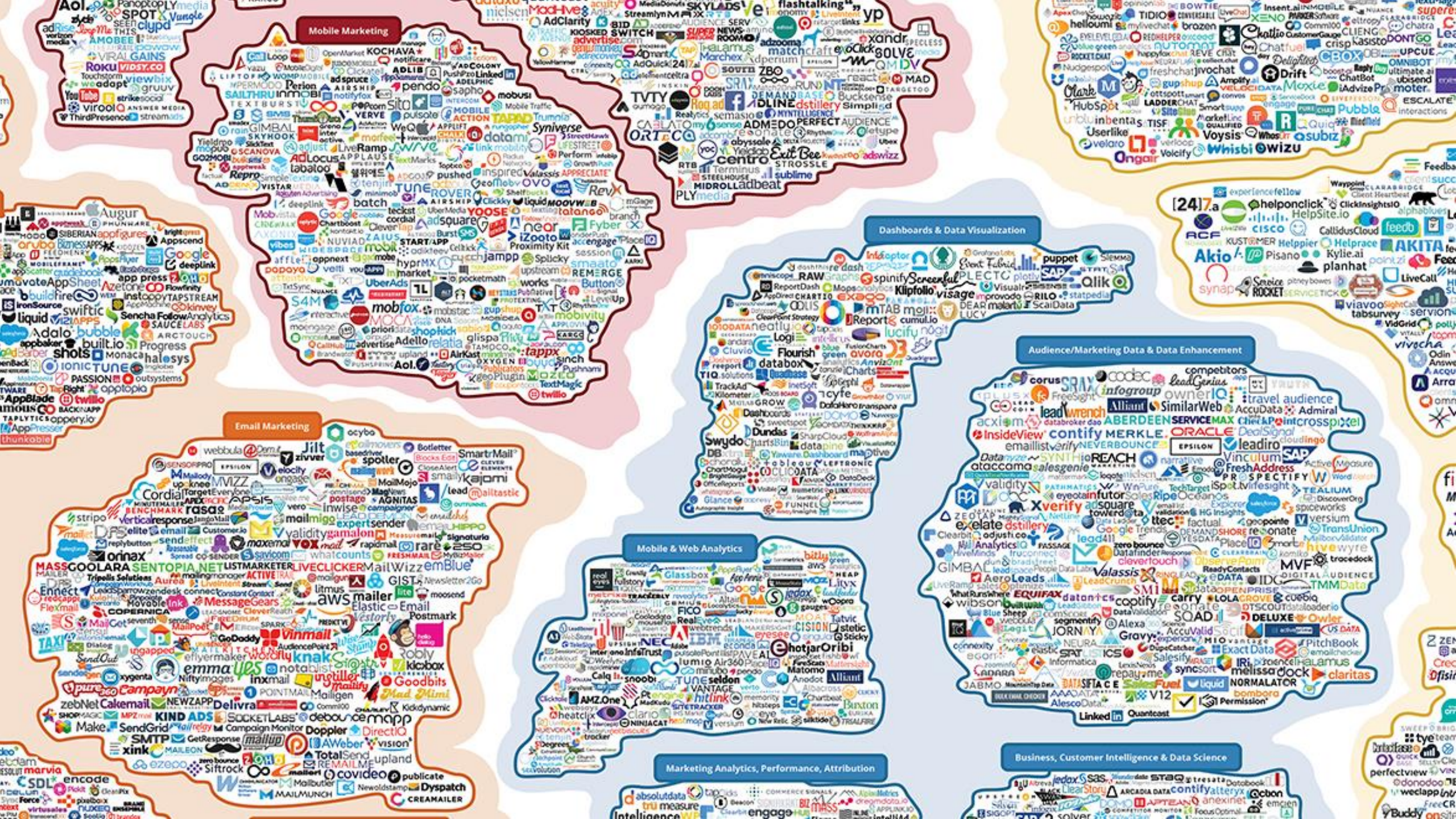
2016
3,874 solutions

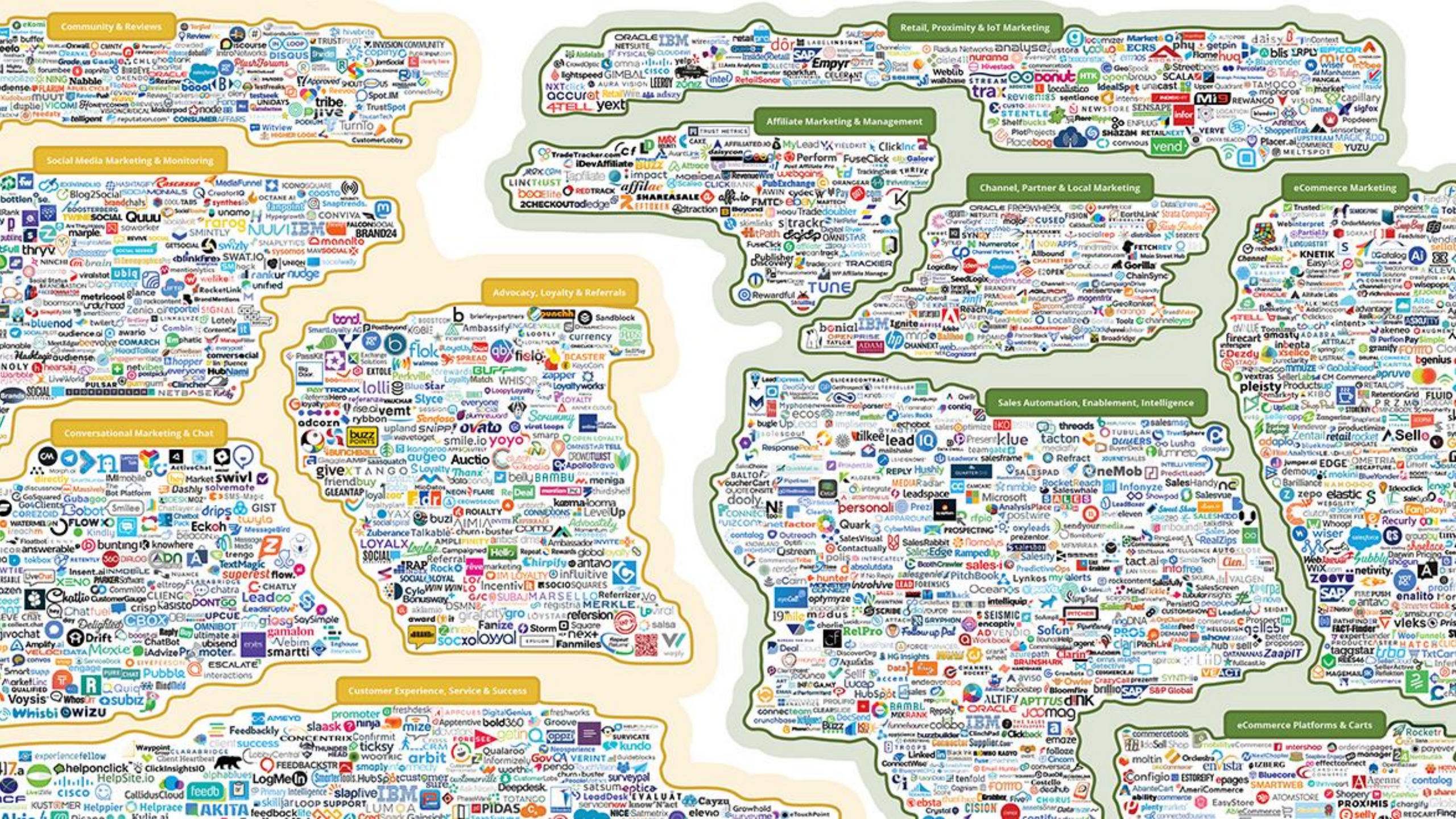
2015
1,876 solutions

2014
947 solutions



Produced by Scott Brinker (@chiefmartec) and Blue Green Brands (@bluegreenbrands).


Mobile Marketing
Dashboards & Data Visualization
Audience/Marketing Data & Data Enhancement
Email Marketing
Mobile & Web Analytics
Marketing Analytics, Performance, Attribution
Business, Customer Intelligence & Data Science

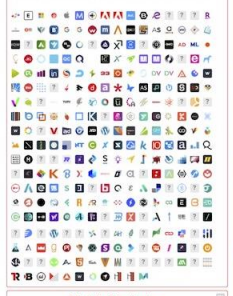

Community & Reviews
Retail, Proximity & IoT Marketing
Affiliate Marketing & Management
Social Media Marketing & Monitoring
Channel, Partner & Local Marketing
eCommerce Marketing
Advocacy, Loyalty & Referrals
Sales Automation, Enablement, Intelligence
Conversational Marketing & Chat
eCommerce Platforms & Carts
Customer Experience, Service & Success

MartechMap an initiative by chiefmartec & MartechTribe

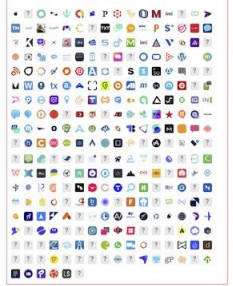
2023 Marketing Technology Landscape May 2023

Advertising and Promotion

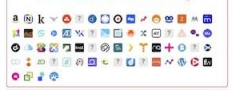
Display & Programmatic Advertising



Mobile Marketing



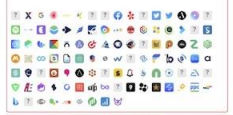
Native/Content Advertising



PR

Print

Search & Social Advertising



Video Advertising

Content and Experience

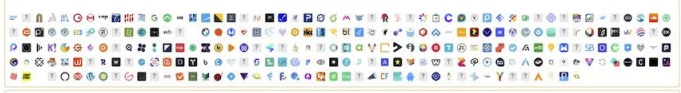
Content Marketing

CMS & Web Experience Management

DAM & MRM & PIM

Email Marketing

Interactive Content



Marketing Automation & Campaign/Lead Management

Mobile Apps

Optimization Personalization & Testing

SEO

Video Marketing

Social and Relationships

ABM

Call Analytics & Management

Customer Experience Service & Success

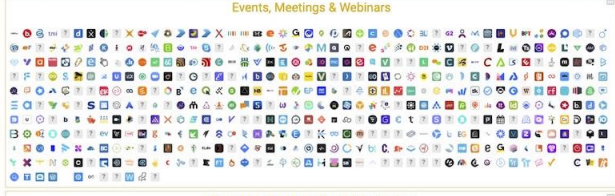
Influencers

CRM

Advocacy Loyalty & Referrals

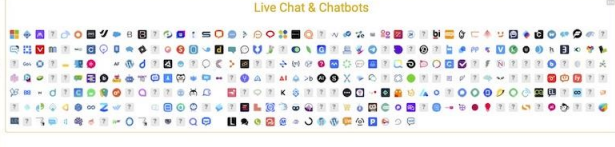
Community & Reviews

Events, Meetings & Webinars



Social Media Marketing & Monitoring

Live Chat & Chatbots



Commerce and Sales

Retail, Proximity & IOT

Affiliate Marketing & Management

Sales Automation Enablement & Intelligence

eCommerce Platforms & Carts

eCommerce Marketing

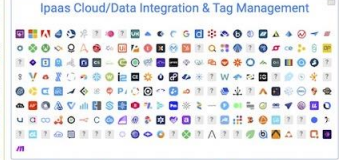
Channel Partner & Local Marketing

Data

Marketing Analytics Performance & Attribution

Audience/Marketing Data & Data Enhancement

Ipaas Cloud/Data Integration & Tag Management



Business/Customer Intelligence & Data Science

DMP

Dashboards & Data Visualization

Governance Compliance And Privacy

Mobile & Web Analytics

Customer Data Platform

Management

Agile & Lean Management

Collaboration

Talent Management

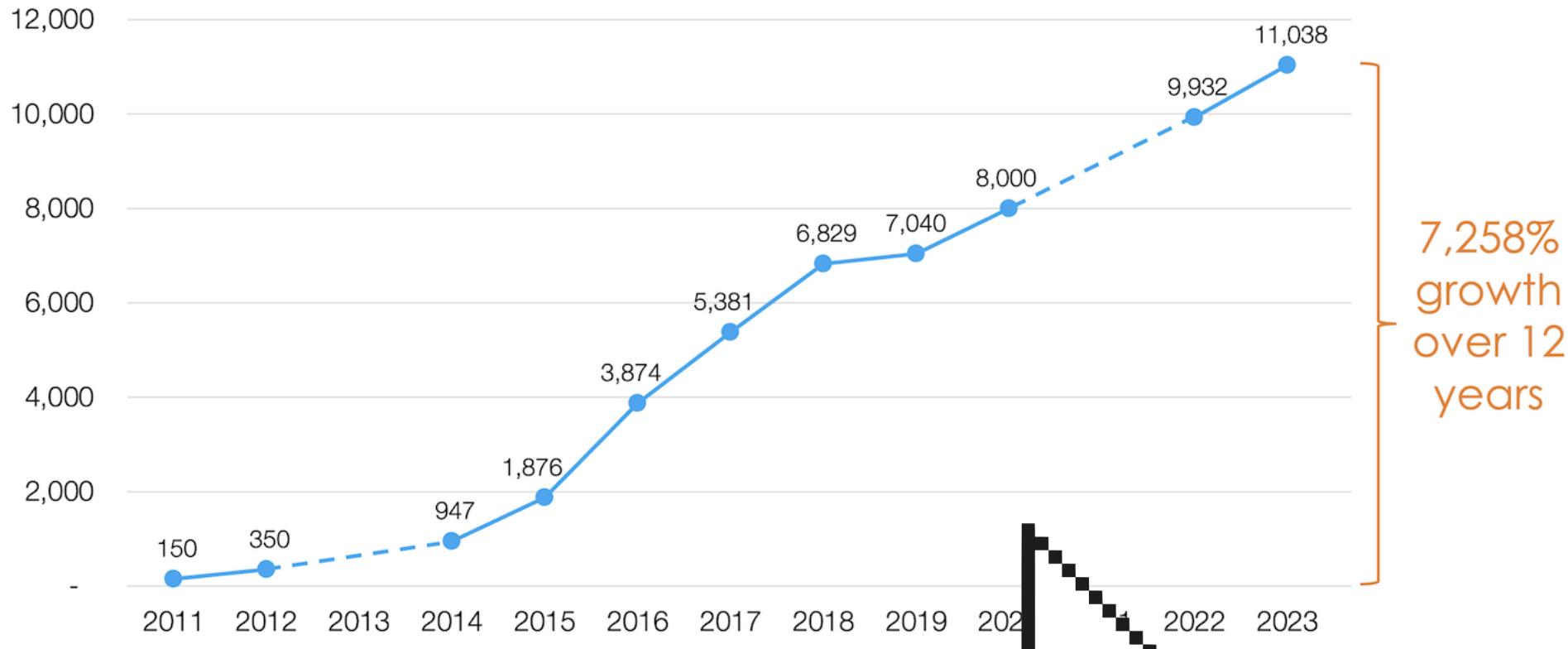
Budgeting & Finance

Projects & Workflow

Product Management

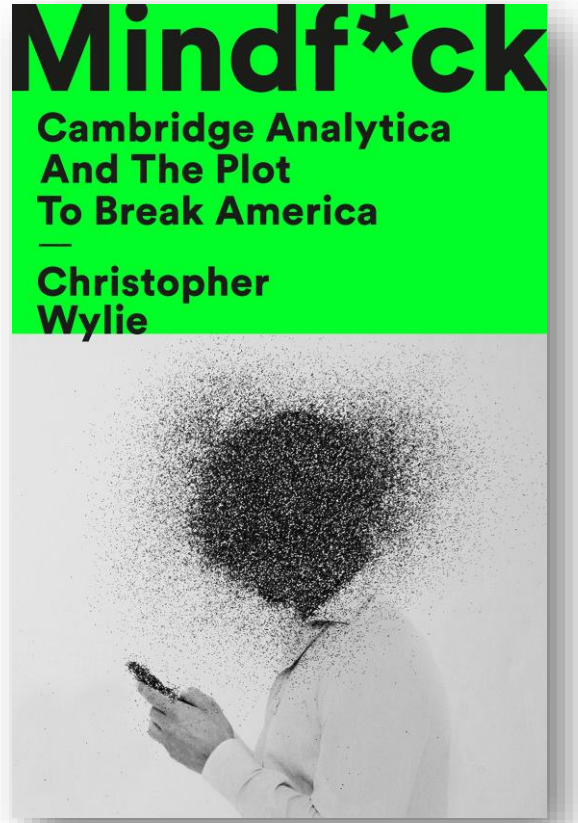
Vendor Analysis & Management

visit martechmap.com to search, sort & filter



remarketing, retargeting...

Cambridge Analytica



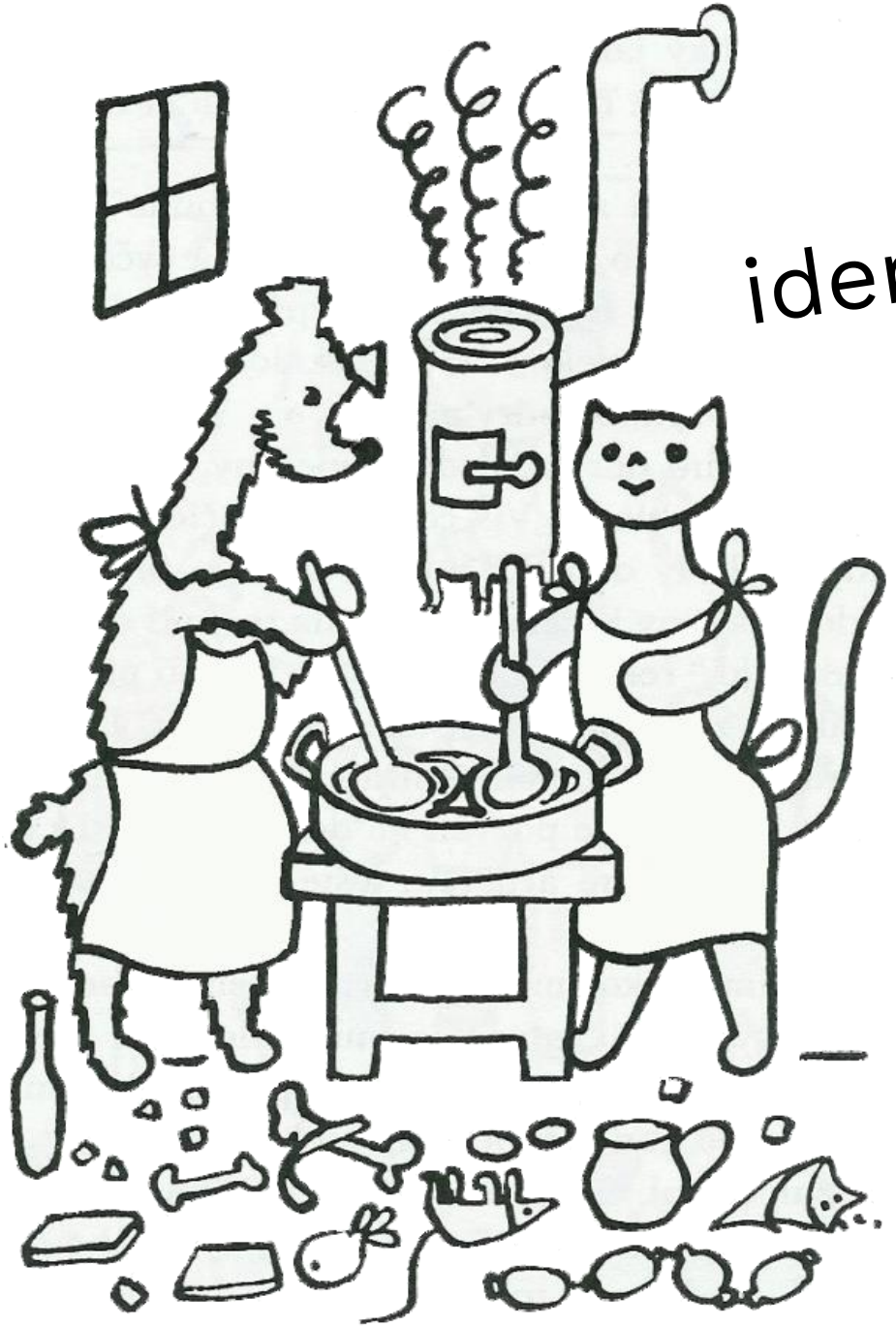
Interaktivní osnova -> DEFCON25: *Dark Data*

Jak můžeme
na internetu/webu
jednoznačně
identifikovat
uživatele?

cookies

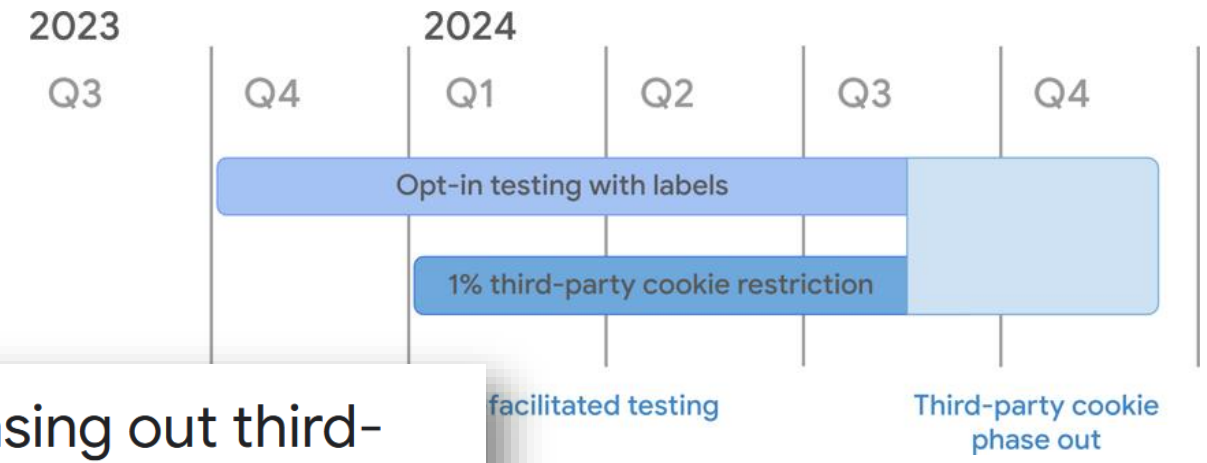
fingerprinting

skripty



identifikátory

Cookies *(třetích stran)*
jsou mrtvá technologie...



Prepare for phasing out third-party cookies

Learn how to audit your code to look for third-party cookies and what action you can take to ensure you're all set for the end of third-party cookies.

Published on Wednesday, May 17, 2023 • Updated on Wednesday, October 11, 2023

Translated to: 日本語

Milica Mihajlija
Milica is a technical writer at Chrome.
Website Twitter GitHub

Third-party cookies are the main mechanism that enables cross-site tracking and several major browsers either already placed restrictions on third-party cookies in some way or are planning to. Third-party cookies also enable many valid use cases such as managing state in embedded content or enabling user sessions across multiple sites.

As part of the Privacy Sandbox project, Chrome is phasing out support for third-party cookies and proposing new functionality for cookies along with purpose-built APIs to continue supporting legitimate use cases while preserving user privacy. The phase out will be gradual, starting from midway through 2024.

Co s tím?

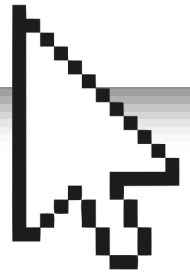
Řešení: Privacy Sandbox

„In the past, third-party cookies and other mechanisms have been used to track user browsing behavior across sites to infer topics of interest. These mechanisms are being phased out as part of the Privacy Sandbox initiative.“

https://privacysandbox.com/

In one, users get to decide what information to share with each site they choose to interact with. No one needs to worry that their past browsing will be held against them—or leveraged to manipulate them—when they next open a tab.

In the other, each user's behavior follows them from site to site as a label, inscrutable at a glance but rich with meaning to those in the know. Their recent history, distilled into a few bits, is "democratized" and shared with dozens of nameless actors that take part in the service of each web page. Users begin every interaction with a confession: here's what I've been up to this week, please treat me accordingly.

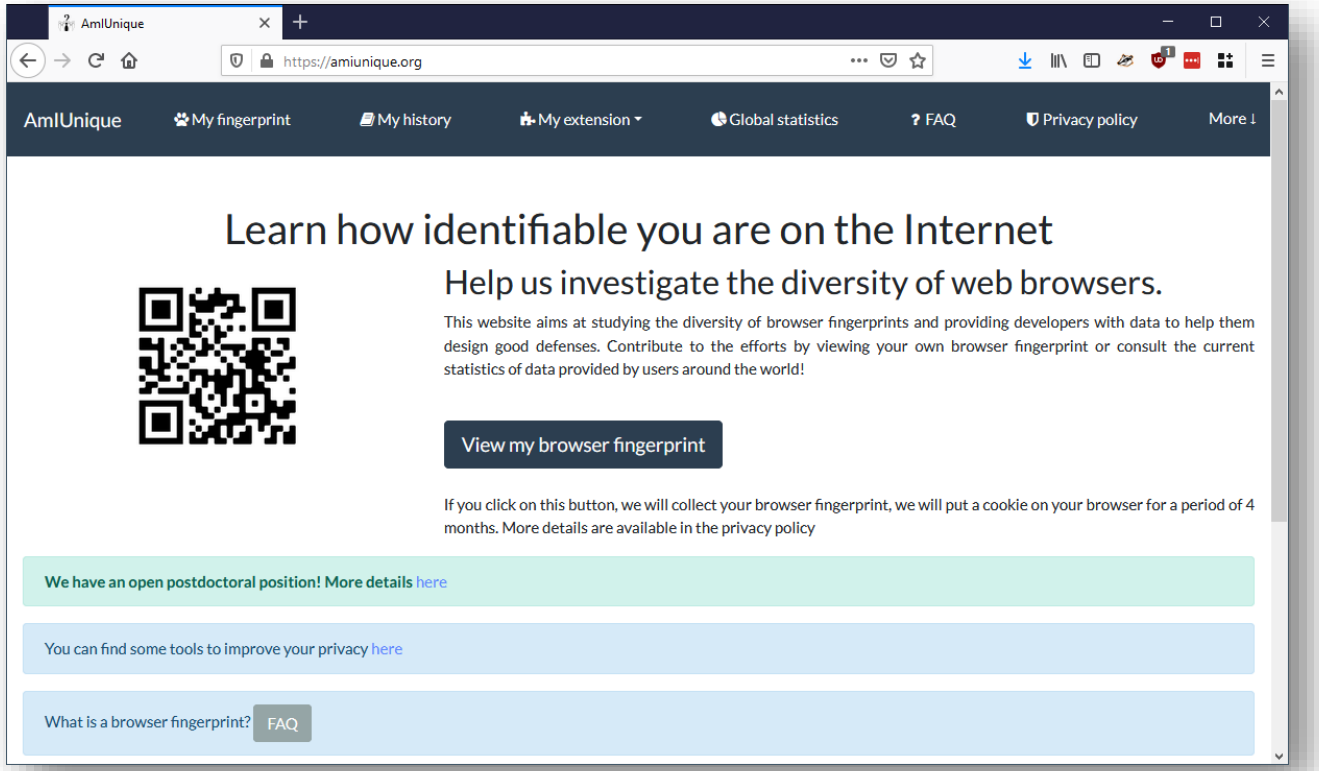


Topics API *vs* FLoC

privacy washing

privacy fixing

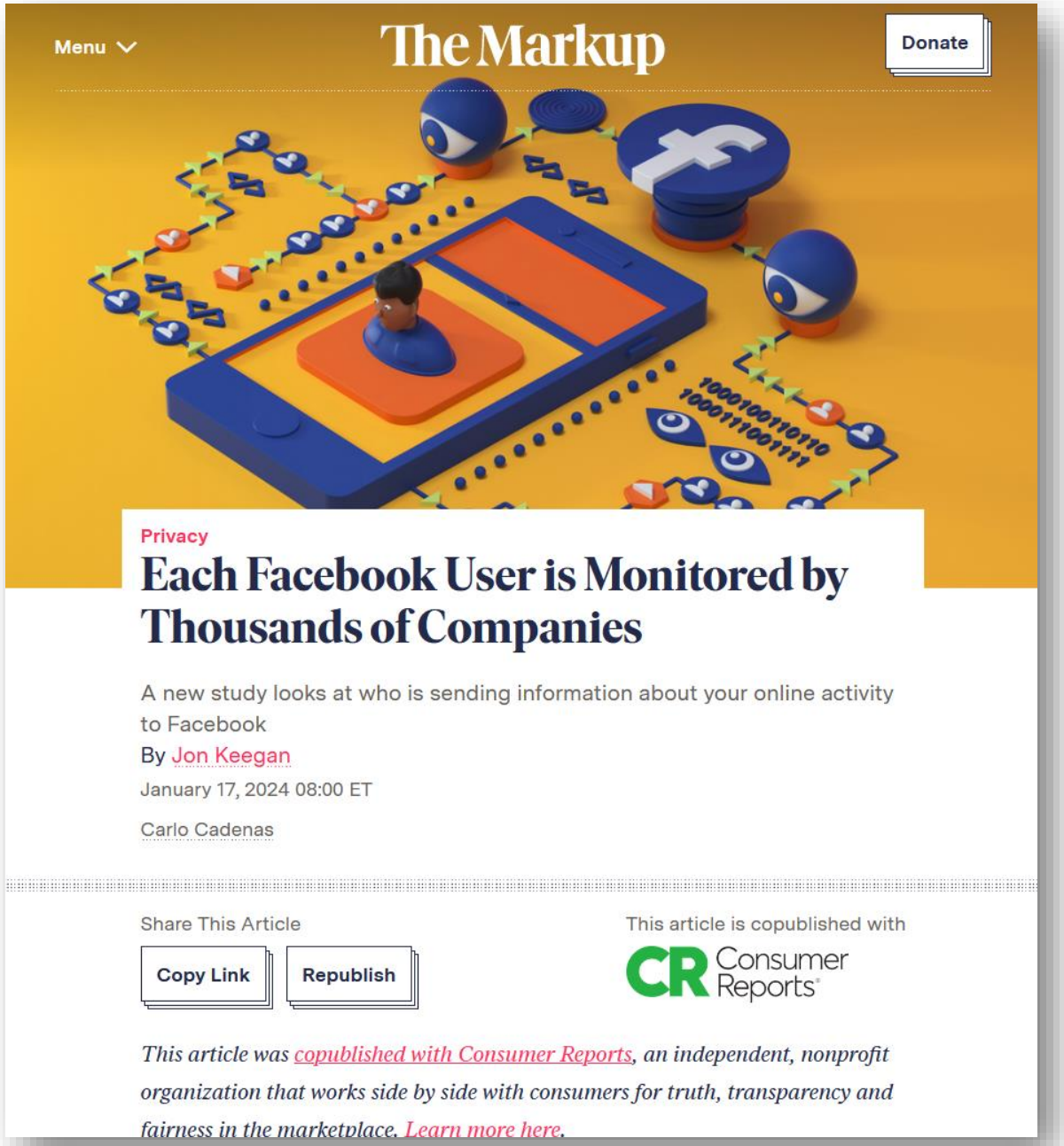
Řešení: Fingerprinting



co s tím?

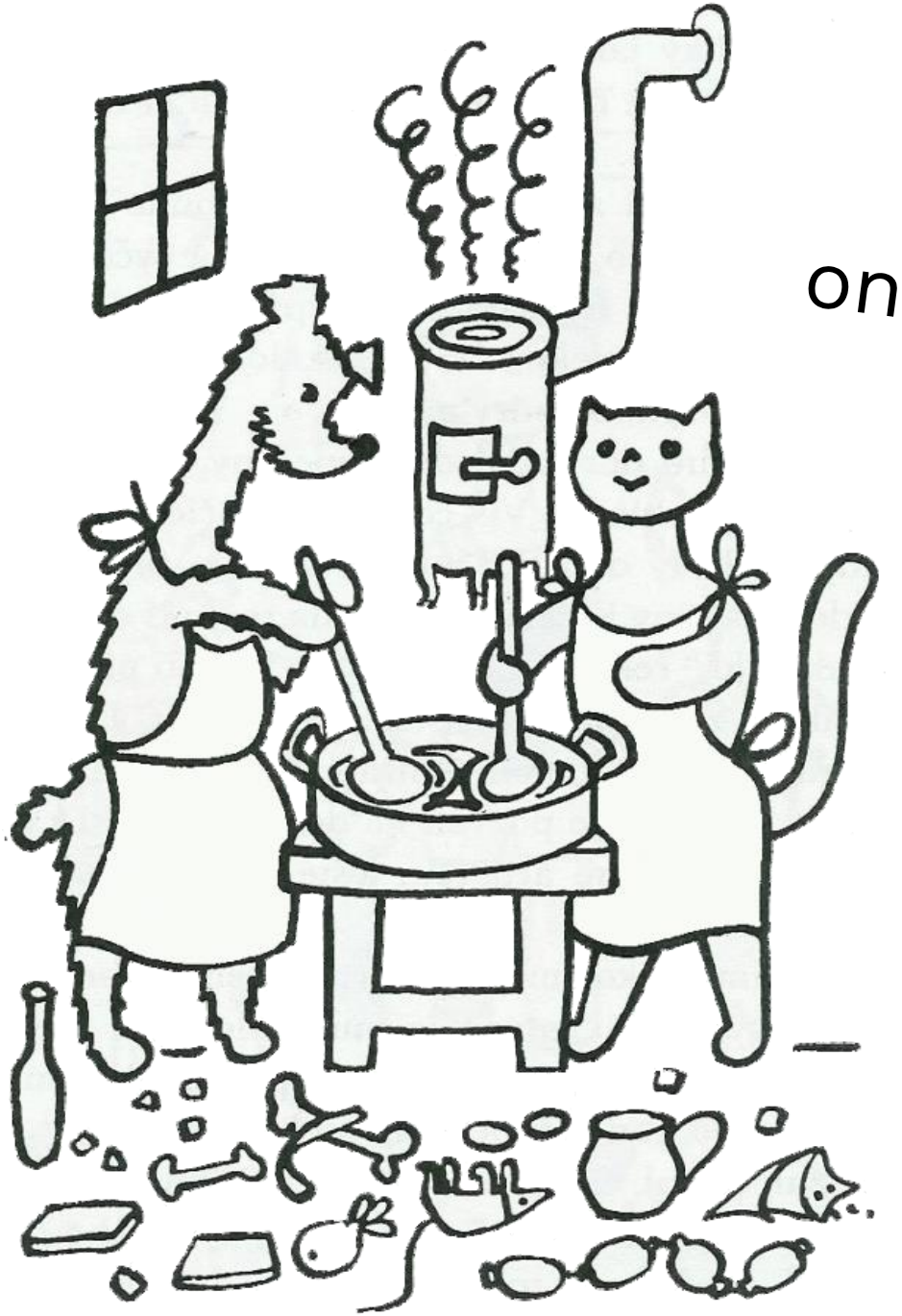
vnášet chaos

Řešení: S2S tracking



HTTPS

onion routing



VPN

HTTPS

- *co je za potíže s HTTP?*
- SSL a certifikace
- šifrované propojení
- HTTPS Everywhere

Vyhláška č. 357/2012 Sb. o uchovávání, předávání a likvidaci provozních a lokalizačních údajů

```
[2022/10/19 16:26] [...]
[2022/10/19 16:30] novinky.cz
[2022/10/19 16:35] idnes.cz
[2022/10/19 16:42] seznam.cz
[2022/10/19 16:43] google.cz
[2022/10/19 17:01] kocarky.cz
[2022/10/19 17:08] mimibazar.cz
[2022/10/19 17:30] google.cz
[2022/10/19 17:33] hnutiprozivot.cz
[2022/10/19 17:37] interupce.info
[2022/10/19 17:39] napocatku.cz
[2022/10/19 17:44] fnbrno.cz
[2022/10/19 18:01] mapy.cz
[2022/10/19 18:07] [...]
```

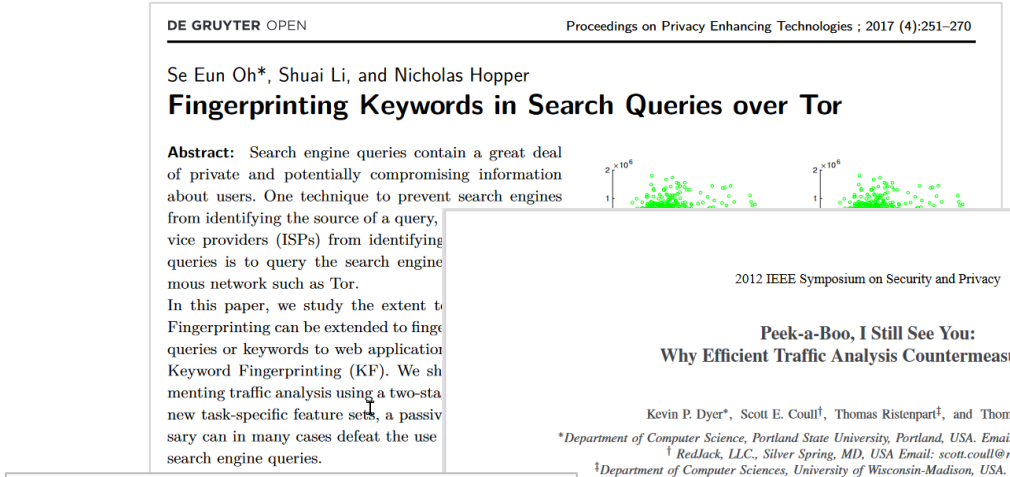
HTTPS

- nejde jen o obsah komunikace
- metadata jsou často mnohem cennější vhled

```
[2020/11/19 17:30] google.cz
[2020/11/19 17:33] hnutiprozivot.cz
[2020/11/19 17:37] interupce.info
[2020/11/19 17:39] napocatku.cz
[2020/11/19 17:44] fnbrno.cz
[2020/11/19 18:01] mapy.cz
```

HTTPS

- *dá se to obejít?*
- *website fingerprinting*
  identifikace jednotlivých stránek
- odhadování *query* podle množství přenášených dat a rychlosti



DE GRUYTER OPEN — Proceedings on Privacy Enhancing Technologies ; 2017 (4):251–270

Se Eun Oh*, Shuai Li, and Nicholas Hopper

Fingerprinting Keywords in Search Queries over Tor

Abstract: Search engine queries contain a great deal of private and potentially compromising information about users. One technique to prevent search engines from identifying the source of a query, vice providers (ISPs) from identifying queries is to query the search engine mous network such as Tor.

In this paper, we study the extent t Fingerprinting can be extended to finge queries or keywords to web applicatio Keyword Fingerprinting (KF). We sh menting traffic analysis using a two-sta new task-specific feature sets, a passiv sary can in many cases defeat the use search engine queries.

2012 IEEE Symposium on Security and Privacy

Peek-a-Boo, I Still See You: Why Efficient Traffic Analysis Countermeasures Fail

Kevin P. Dyer*, Scott E. Coull†, Thomas Ristenpart‡, and Thomas Shrimpton*

*Department of Computer Science, Portland State University, Portland, USA. Email: {kdyer, teshrim}@cs.pdx.edu
† RedJack, LLC., Silver Spring, MD, USA Email: scott.coull@redjack.com
‡Department of Computer Sciences, University of Wisconsin-Madison, USA. Email: rist@cs.wisc.edu

ract—
consider the setting of HTTP traffic over encrypted , as used to conceal the identity of websites visited ser. It is well known that traffic analysis (TA) attacks curately identify the website a user visits despite the encryption, and previous work has looked at specific countermeasure pairings. We provide the first com- sive analysis of general-purpose TA countermeasures. w that nine known countermeasures are vulnerable to attacks that exploit coarse features of traffic (e.g., to- e and bandwidth). The considered countermeasures ones like those standardized by TLS, SSH, and and even more complex ones like the traffic morphing of Wright et al. As just one of our results, we show spite the use of traffic morphing, one can use only pstream and downstream bandwidth to identify — % accuracy— which of two websites was visited. One tion of what we find is that, in the context of website cation, it is unlikely that bandwidth-efficient, general- e TA countermeasures can ever provide the type of y targeted in prior work.

***words*-traffic analysis countermeasures; privacy; ma- earning; padding; encrypted traffic**

I. Introduction

rnet users increasingly rely on encrypted tunnels to heir web browsing activities safe from eavesdrop- A typical scenario involves a user establishing an ted tunnel to a proxy that then relays all subsequent

manipulate whole streams of packets in order to precisely mimic the distribution of another website's packet lengths.

The seemingly widespread intuition behind these countermeasures is that they patch up the most dangerous side channel (packet lengths) and so provide good protection against TA attacks, including website identification. Existing literature might appear to support this intuition. For example, Liberatore and Levine [10] show that padding packets to the network MTU (e.g., 1500 bytes) reduces the accuracy of one of their attacks from 98% to 7%.

Our results strongly challenge this intuition. We perform the first comprehensive analysis of low-level countermeasures (e.g., per-packet padding) for the kind of website identification attacks considered by prior work (c.f., [8, 10, 14, 22]): a closed-world setting for privacy sets, in which the *a priori* set of possible websites a user might visit is known to the attacker, coupled with the ability for the attacker to train and test on traffic traces that are free of real-world artifacts (e.g., caching effects, interleaved flows, and user-specific content). We consider nine distinct countermeasures, apply them to two large, independent datasets of website downloads, and pit the resulting obfuscated traffic against a total of seven different attacks. The results are summarized in Figure 1. What we uncover is surprisingly bleak:

None of the countermeasures are effective. We show

RESEARCH-ARTICLE

Touching from a distance: website fingerprinting attacks and defenses

AddThis

Authors: Xiang Cai, Xin Cheng Zhang, Brijesh Joshi, Rob Johnson Authors Info & Affiliations

Publication: CCS '12: Proceedings of the 2012 ACM conference on Computer and communications security • October 2012 • Pages 605–616 • https://doi.org/10.1145/2382196.2382260

112 1,216 Get Access

ABSTRACT

We present a novel web page fingerprinting attack that is able to defeat several recently proposed defenses against traffic analysis attacks, including the application-level defenses HTTPOS and randomized pipelining over Tor. Regardless of the defense scheme, our attack was able to guess which of 100 web pages a victim was visiting at least 50% of the time and, with some defenses, over 90% of the time. Our attack is based on a simple model of network behavior and out-performs previously proposed ad hoc attacks. We then build a web site fingerprinting attack that is able to identify whether a victim is visiting a particular web site with over 90% accuracy in our experiments.

VPN

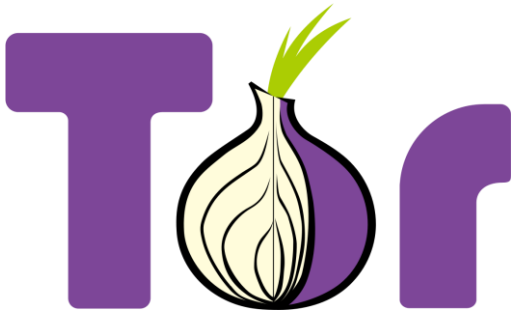
- důležitým identifikátorem je IP adresa
- *virtuální privátní síť* – k čemu to je?

- *jaké to má potíže?*
- zdarma = pomalé a *no*-no-log policy
- přenášení důvěry *(ISP -> VPN poskytovatel)*

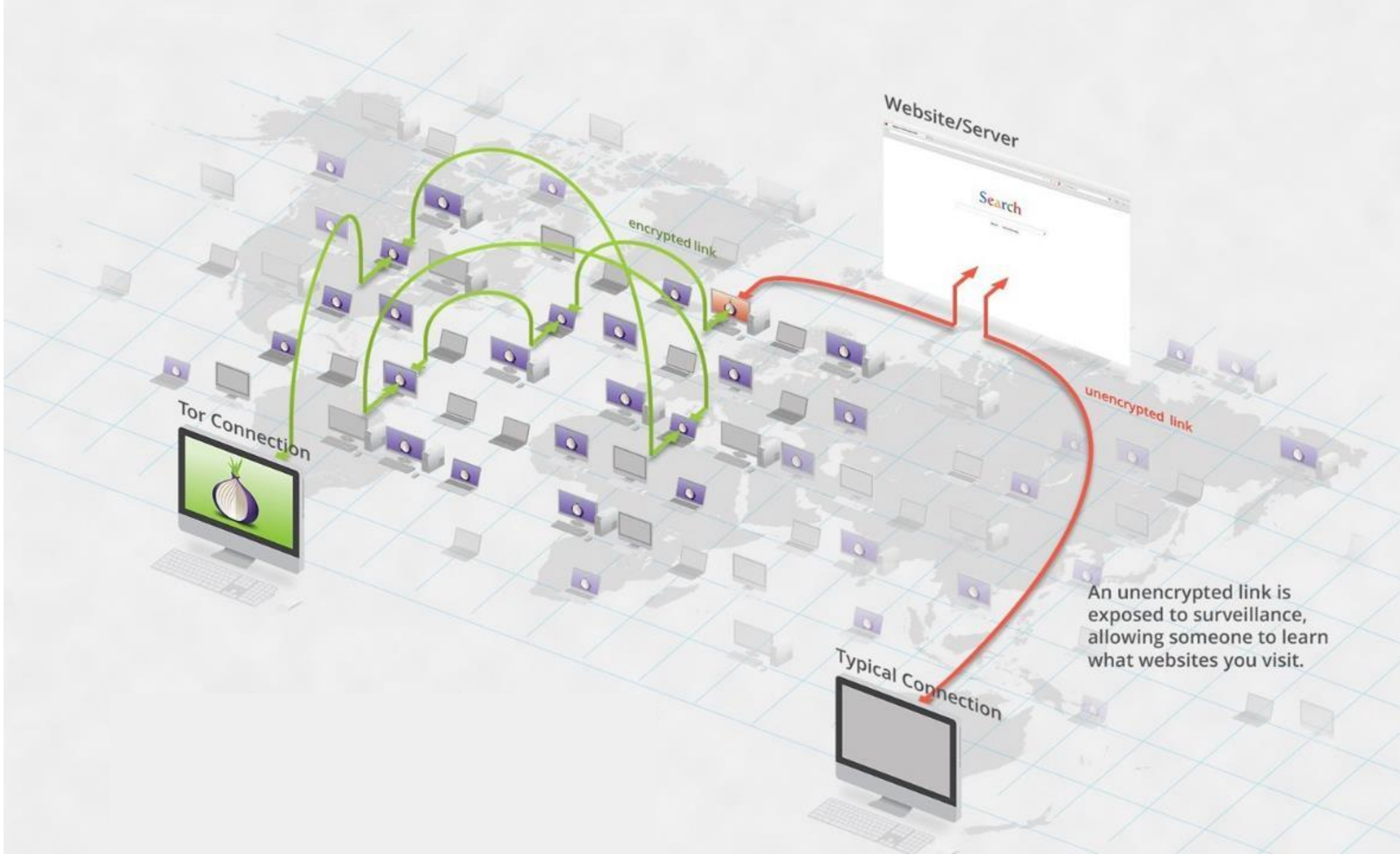
Onion routing

- původ v armádním výzkumu
- vytvořit spojení, které neprozradí kdo s kým mluví
- nosnou myšlenkou byl onion routing
- MIT *(2000)* – výzkumy *Tor* (The Onion Routing)
- fungování založeno na decentralizované síti
- *proč je vojenská technologie dostupná všem?*

Tor



- potřeba uzlů: otevřeno (2002)
- 2004 – podpora EFF
- ALE: technologická náročnost
- Tor Browser (2008) – klientský SW
- 2010 – Arabské jaro *(ochrana identity, přístup)*
- 2013 – kauza Snowden


Website/Server
Search
encrypted link
unencrypted link
Tor Connection
Typical Connection
An unencrypted link is exposed to surveillance, allowing someone to learn what websites you visit.

Tor není darkweb!

HANSA

Home | Lotteries | Forums | Support | Login | Register

Categories

- Drugs 18836
- Fraud Related 2026
- Guides & Tutorials 3702
- Services 1431
- Jewellery 54
- Digital Goods 12425
- Erotica 1396
- Counterfeits 683
- Electronics 33
- Security & Hosting 90
- Miscellaneous 312

Welcome to HANSA Market

The Darknet Market with the main focus on a trustless payment system, which makes it impossible for the vendors OR the site staff to run away with Bitcoins of the buyers.

Multisig escrow

Optional 2-of-3 multisig for buyers and 2-of-2 multisig as a fallback for buyers that do not want to bother with multi-signature. Money can never be accessed by the market staff. Theft is impossible.

No Bitcoin deposits

Every order has its unique Bitcoin address similar to BitPay's or Coinbase's payment system. Buyers have 15 minutes to pay the order and do not have to wait for deposits to arrive.

No Finalize Early

We do not support FE or partial escrow releases and we don't have to! The multisignature escrow makes it impossible for the site staff or vendors to steal any Bitcoins.

Current Lottery Jackpot: Ƀ 8.4545 USD 21,635.72 Buy tickets

Featured Listings

USD 11.35
Ƀ 0.0044

0.2G Sample - 80% Pure Bolivian Cocaine (Levamisole Free) (Free shipping) 10 €

AmsterdamSupply [+8|0]

Level 2 (9)

USD 199.00
Ƀ 0.0778

100 XTC Pill 230mg (MDMA) 84% ★ PINK DONALD TRUMP FACE ★ ONLY USA ★ SPECIAL DISCOUNT

DreamShop [+588|0]

★ Level 9 (800+)

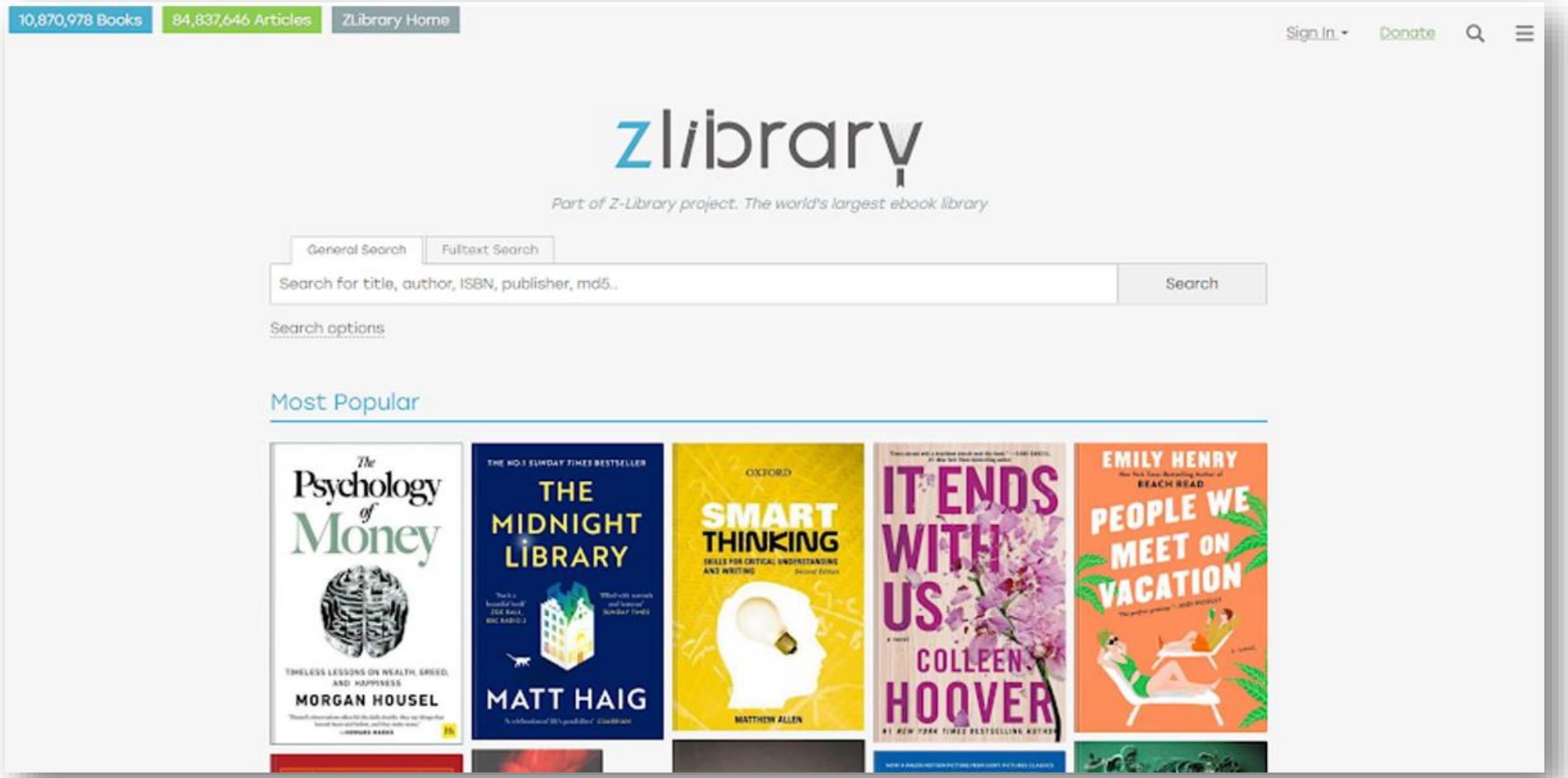
USD 150.99
Ƀ 0.059

100 - Xanax Pfizer X2 Replicas 3mg Alprazolam - US2US - Tracked

StarkoftheNorth [+1|0]

★ Level 1 (1)

operational security


10,870,978 Books
84,837,646 Articles
ZLibrary Home
Sign In
Donate
zlibrary
Part of Z-Library project. The world's largest ebook library
General Search
Fulltext Search
Search for title, author, ISBN, publisher, md5..
Search
Search options
Most Popular
The Psychology of Money
MORGAN HOUSEL
THE MIDNIGHT LIBRARY
MATT HAIG
OXFORD
SMART THINKING
MATTHEW ALLEN
IT ENDS WITH US
COLLEEN HOOVER
EMILY HENRY
PEOPLE WE MEET ON VACATION

On November 16, 2022, U.S. Attorneys for the Eastern District of New York of the Department of Justice unsealed the indictment for two Russian nationals: Anton Napolsky and Valeriia Ermakova, who had been arrested in Argentina on November 3, 2022.[33] They were charged with criminal copyright infringement, wire fraud and money laundering for operating the Z-Library website.[34][35][36] The indictment pertains to alleged criminal activity taking place from 2018 to 2022, though the pair are suspected to have operated Z-Library for "over a decade".[37] Based on details laid out in the criminal complaint, the arrests were accomplished by the FBI with data from Google and Amazon (among other sites), accessed with search warrants, that helped identify the founders of the website.[38] The U.S. lawyers retained as official representatives[39] requested a dismissal of the criminal indictment in June 2023.[40]

When the domains z-lib.org, b-ok.org, and 3lib.net were seized, the DNS servers utilised switched to NS1.SEIZEDSERVERS.COM and NS2.SEIZEDSERVERS.COM, used commonly in US law enforcement seizures. However, these DNS servers have switched to Njalla, an anonymous hosting provider.[14] The website continued to be active and accessible through the Tor network and the I2P network,[25][30][16] before returning to the regular Internet through private personal domains issued to each user on February 11, 2023.[31][32]

14. Google records reflect that a Russian-based telephone number ending in - 2458 ("Napolsky Phone-1") was used to register the email Napolsky7@gmail.com as well as the emails donation.zlib@gmail.com, zlibdoms@gmail.com and feedback.bookos@gmail.com.

15. Google records also reflect that the account associated with the email address feedback.bookos@gmail.com was created with the name "Z-Library Team" and feedback.bookos@gmail.com is the recovery e-mail for the account zlibsupp@gmail.com, which was created with the name "ZLibrary Support." Similarly, zlibsupp@gmail.com is the recovery e-mail account associated with the email address zlibdonat@gmail.com, that was created with the name "Zlibrary Mailer."

ss internet connection) was used to log in to all three accounts.

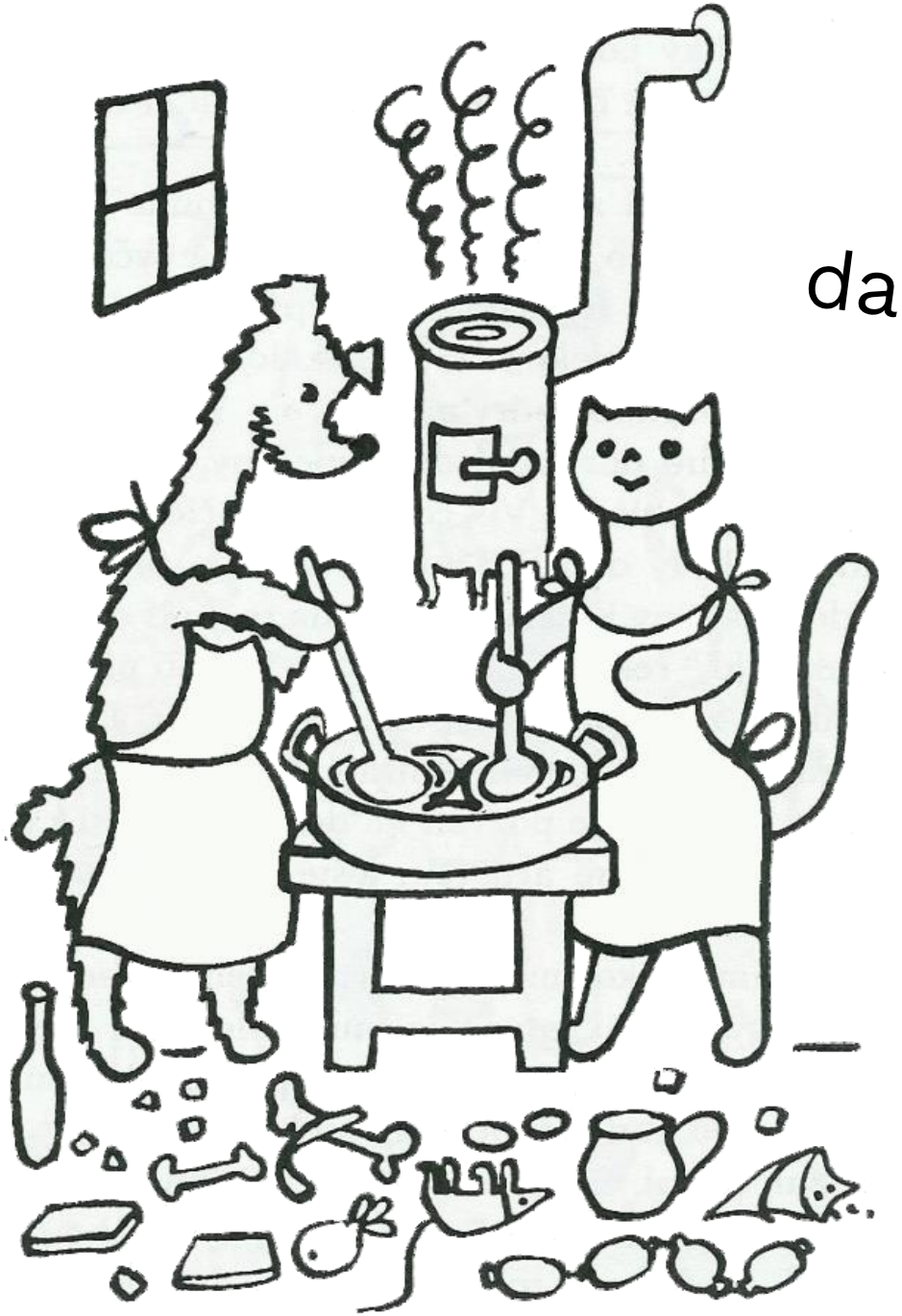
nts logged in from the IP address 5.8.39.0 as indicated below:

	Time Stamp
	10/27/2021 8:48:31 AM
	10/27/2021 8:55:31 AM
Ermakova Personal Email-1	10/27/2021 8:55:31 AM
zlibsupp@gmail.com	10/27/2021 8:55:31 AM
feedback.bookos@gmail.com	10/30/2021 9:49:14 PM
zlibsupp@gmail.com	10/30/2021 9:49:39 PM
Ermakova Personal Email-1	10/30/2021 9:49:39 PM
Ermakova Personal Email-1	10/31/2021 8:58:57 AM
zlibsupp@gmail.com	10/31/2021 8:58:58 AM
Ermakova Personal Email-1	11/3/2021 3:33:39 PM
zlibsupp@gmail.com	11/3/2021 3:33:36 PM
Ermakova Personal Email-1	11/6/2021 11:13:14 AM
zlibsupp@gmail.com	11/6/2021 11:13:15 AM
Ermakova Personal Email-1	11/7/2021 8:23:02 PM
zlibsupp@gmail.com	11/7/2021 8:23:03 PM

Anonymní OS

- nejvyšší level
- všechno v jednom
- běží z CD nebo USB
- nezanechává stopu v PC
- https://tails.boum.org/

platformy



data breach

backdoors

Náš obsah leží jinde

- *Gmail, Facebook,...*
- přístup k vlastním datům?
- kontrola nad daty?
- nastavení soukromí?
- data leaks / breach
- have i been pwned?

Oh no — pwned!

Pwned in 26 data breaches and found 4 pastes (subscribe to search sensitive breaches)

Donate

Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public.

500px: In mid-2018, the online photography community 500px suffered a data breach. The incident exposed almost 15 million unique email addresses alongside names, usernames, genders, dates of birth and either an MD5 or bcrypt password hash. In 2019, the data appeared listed for sale on a dark web marketplace (along with several other large breaches) and subsequently began circulating more broadly. The data was provided to HIBP by a source who requested it to be attributed to "BenjaminBlue@exploit.im".

Compromised data: Dates of birth, Email addresses, Genders, Geographic locations, Names, Passwords, Usernames

Adobe: In October 2013, 153 million Adobe accounts were breached with each containing an internal ID, username, email, *encrypted* password and a password hint in plain text. The password cryptography was poorly done and many were quickly resolved back to plain text. The unencrypted hints also disclosed much about the passwords adding further to the risk that hundreds of millions of Adobe customers already faced.

Compromised data: Email addresses, Password hints, Passwords, Usernames

Animoto: In July 2018, the cloud-based video making service Animoto suffered a data breach. The breach exposed 22 million unique email addresses alongside names, dates of birth, country of origin and salted password hashes. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".

Compromised data: Dates of birth, Email addresses, Geographic locations, Names, Passwords

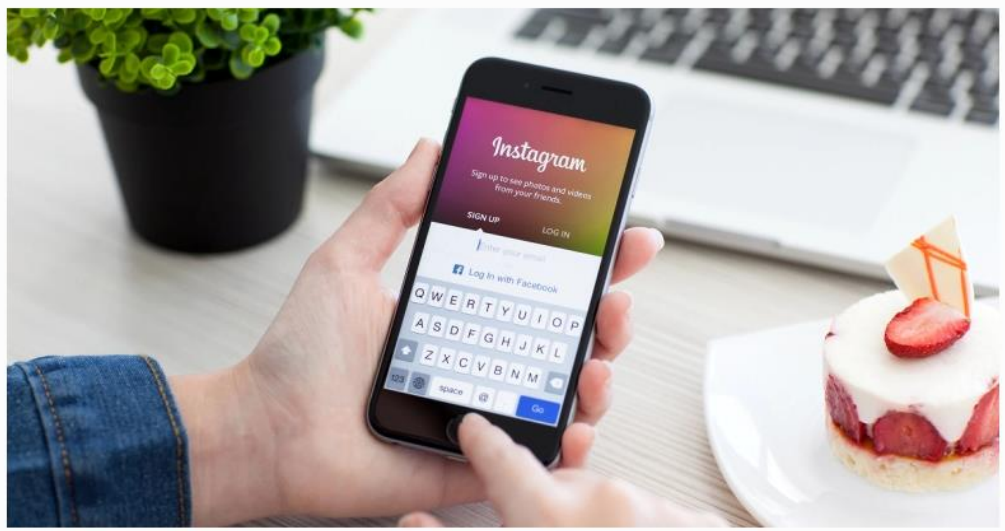
Co se stane po úniku dat?

- objeví se to venku
- často náhodně, často až po čase
- mnohdy k zakoupení
- začne se zkoušet, testovat, kombinovat
- ověřuje se pravdivost a aktuálnost
- *hledá se zdroj* – mnohdy kombinace
- reportuje se

Instagram bug could have allowed others to read your direct messages

17 FEB 2016 3

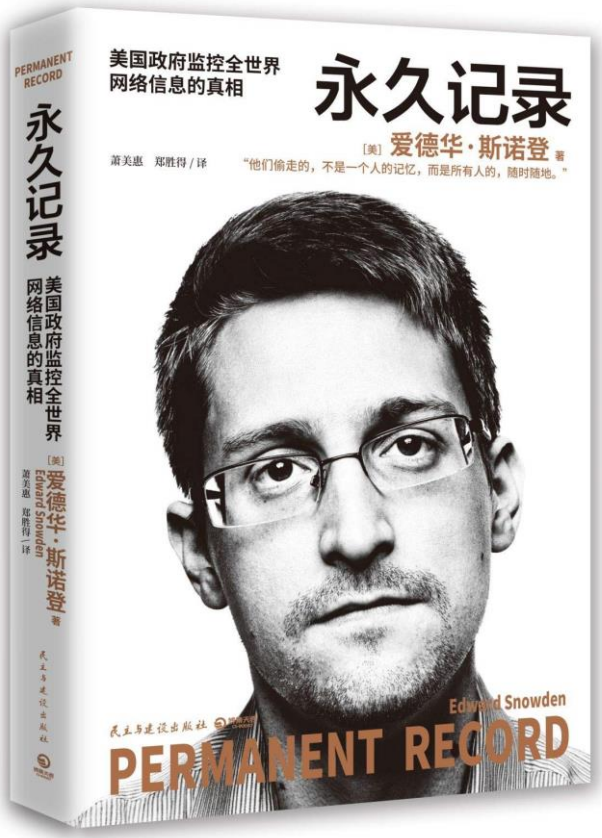
Privacy, Social networks



Previous: "Locky" ransomware – what you need to know

Next: Apple says NO to iPhone backdoor in terror case

backdoor


PERMANENT RECORD
永久记录
美国政府监控全世界网络信息的真相
[美]爱德华·斯诺登 著
Edward Snowden
萧美惠 郑胜得 / 译
"他们偷走的，不是一个人的记忆，而是所有人的，随时随地。"
Edward Snowden
PERMANENT RECORD

TOP SECRET//SI//ORCON//NOFORN

PRISM/US-984XN Overview

OR

*The SIGAD Used **Most** in NSA Report*
Overview

[redacted]

April 2013

Derive

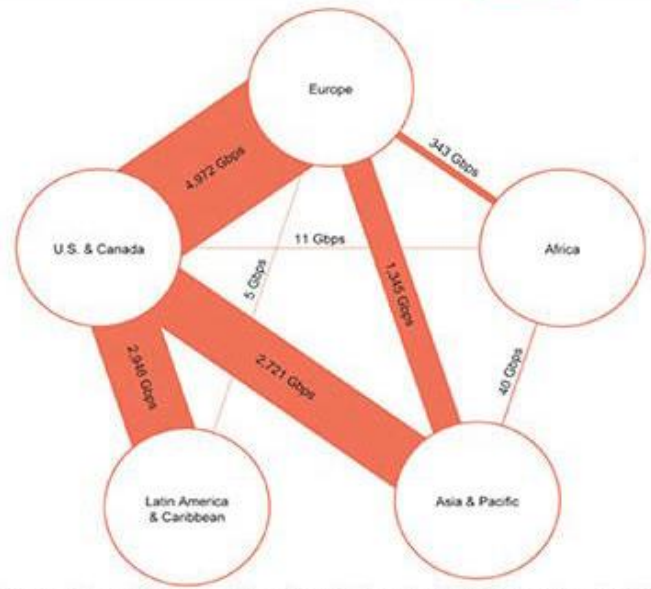
TOP SECRET//S

TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF) Introduction

U.S. as World's Telecommunications Backbone

- Much of the world's communications flow through the U.S.
- A target's phone call, e-mail or chat will take the **cheapest** path, **not the physically most direct** path – you can't always predict the path.
- Your target's communications could easily be flowing into and through the U.S.



International Internet Regional Bandwidth Capacity in 2011
Source: Telegeography Research

TOP SECRET//SI//ORCON//NOFORN

TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF) FAA702 Operations

Two Types of Collection

Upstream

- Collection of communications on fiber cables and infrastructure as data flows past.

(FAIRVIEW, STORMBREW, BLARNEY, OAKSTAR)

You Should Use Both

PRISM

- Collection directly from the servers of these U.S. Service Providers: Microsoft, Yahoo, Google Facebook, PalTalk, AOL, Skype, YouTube Apple.

TOP SECRET//SI//ORC

TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF) PRISM Collection Details

Current Providers

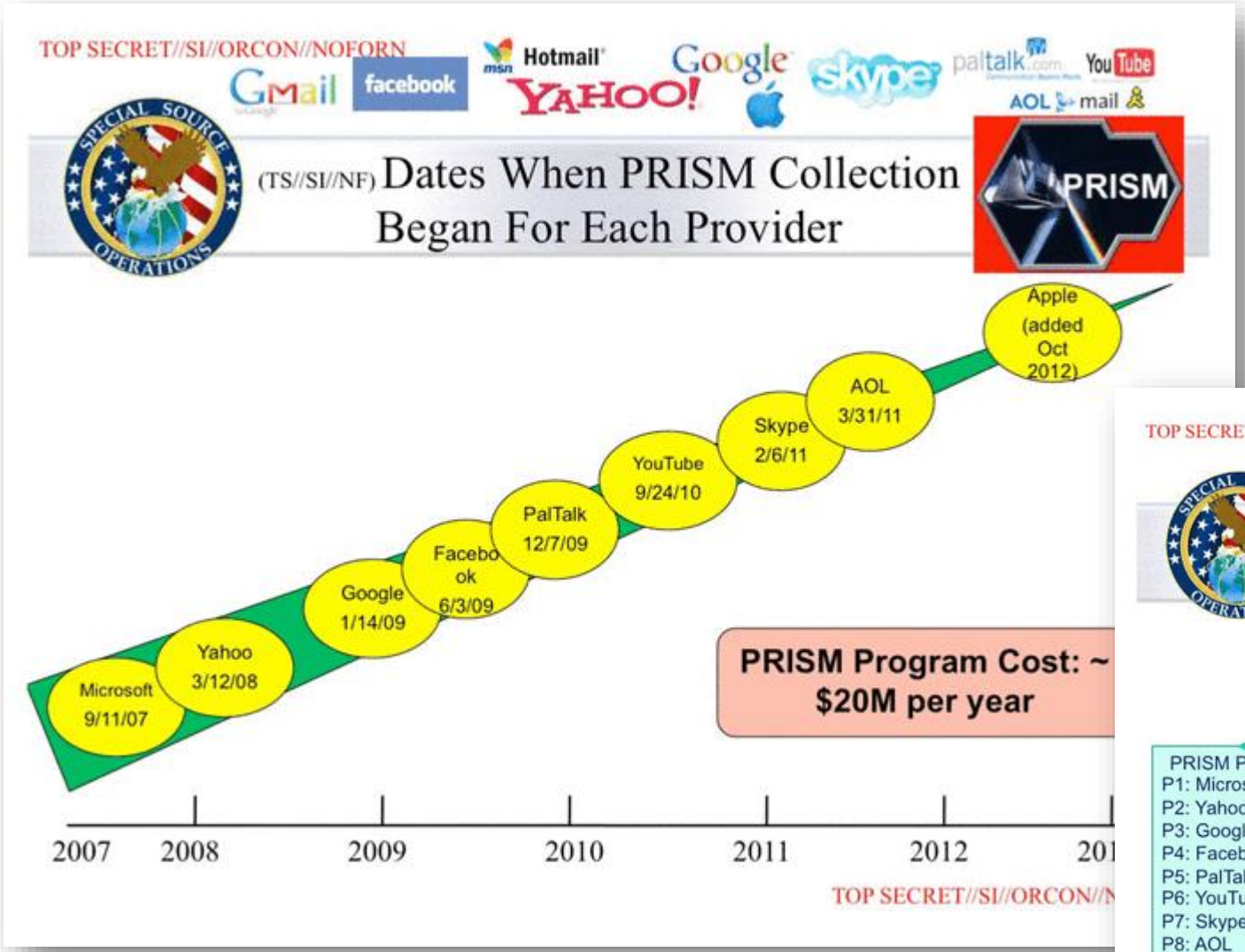
- Microsoft (Hotmail, etc.)
- Google
- Yahoo!
- Facebook
- PalTalk
- YouTube
- Skype
- AOL
- Apple

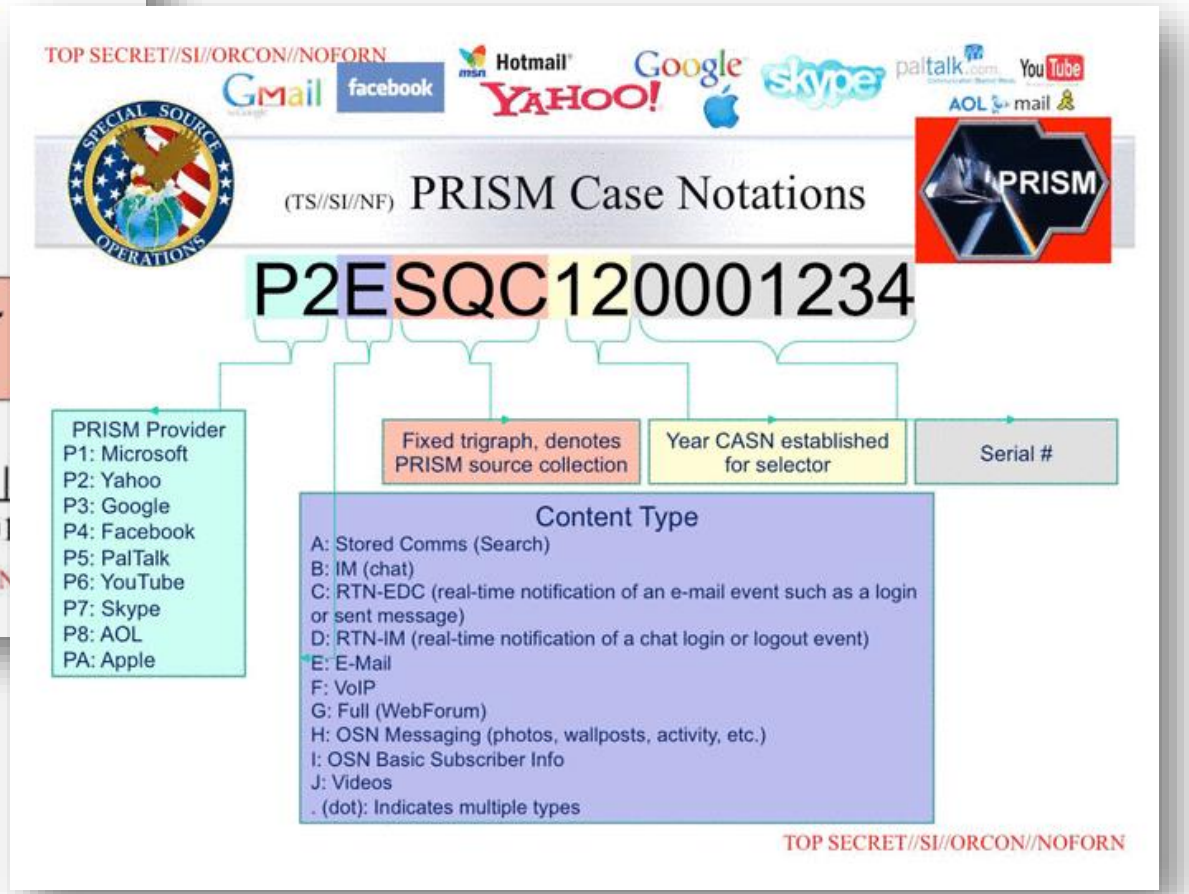
What Will You Receive in Collection (Surveillance and Stored Comms)?
It varies by provider. In general:

- E-mail
- Chat – video, voice
- Videos
- Photos
- Stored data
- VoIP
- File transfers
- Video Conferencing
- Notifications of target activity – logins, etc.
- Online Social Networking details
- **Special Requests**

Complete list and details on PRISM web page:
Go PRISMFAA

TOP SECRET//SI//ORCON//NOFORN

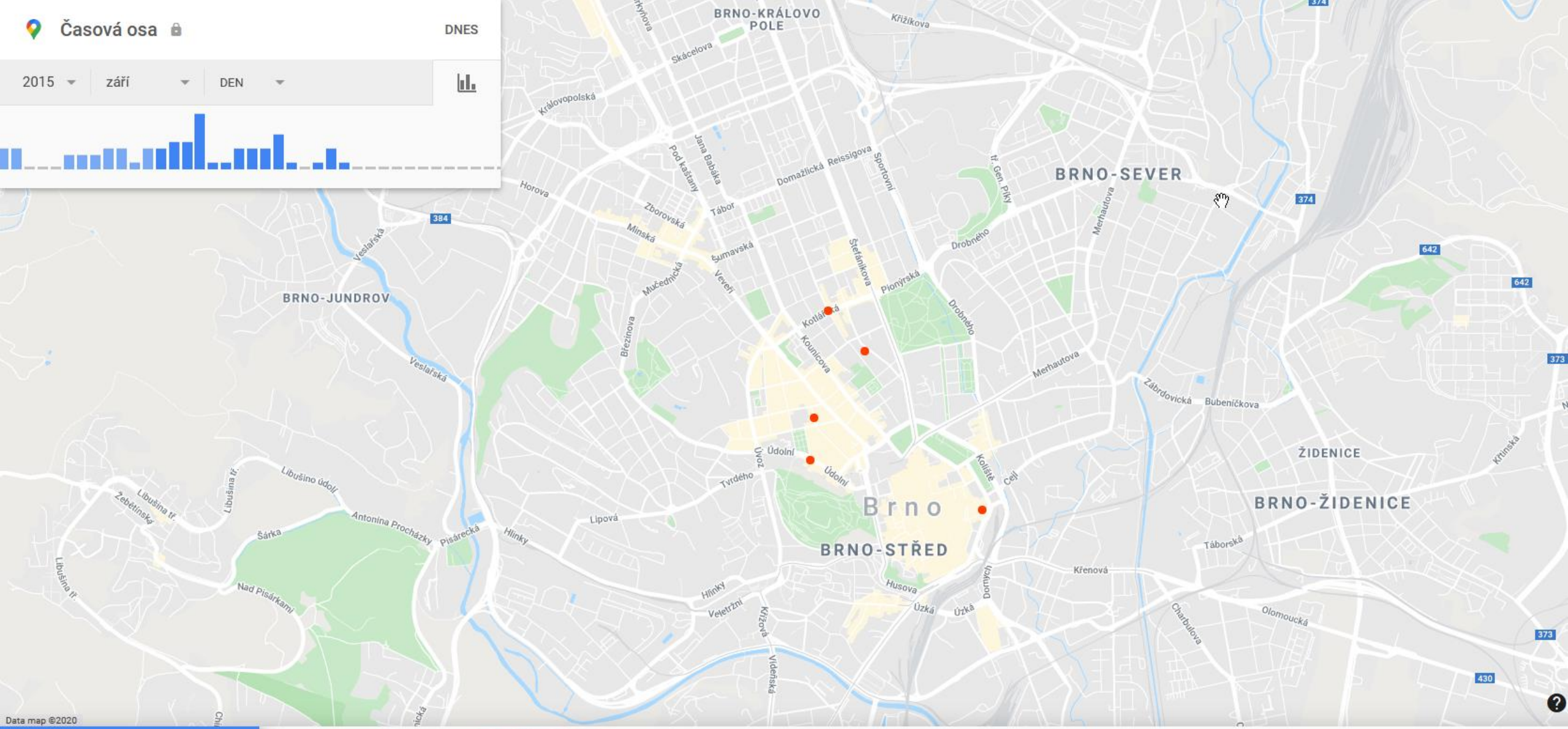

TOP SECRET//SI//ORCON//NOFORN
(TS//SI//NF) Dates When PRISM Collection Began For Each Provider
PRISM
Microsoft 9/11/07
Yahoo 3/12/08
Google 1/14/09
Facebook 6/3/09
PalTalk 12/7/09
YouTube 9/24/10
Skype 2/6/11
AOL 3/31/11
Apple (added Oct 2012)
PRISM Program Cost: ~ $20M per year
2007
2008
2009
2010
2011
2012
TOP SECRET//SI//ORCON//N


TOP SECRET//SI//ORCON//NOFORN
(TS//SI//NF) PRISM Case Notations
PRISM
P2ESQC120001234
PRISM Provider
P1: Microsoft
P2: Yahoo
P3: Google
P4: Facebook
P5: PalTalk
P6: YouTube
P7: Skype
P8: AOL
PA: Apple
Fixed trigraph, denotes PRISM source collection
Year CASN established for selector
Serial #
Content Type
A: Stored Comms (Search)
B: IM (chat)
C: RTN-EDC (real-time notification of an e-mail event such as a login or sent message)
D: RTN-IM (real-time notification of a chat login or logout event)
E: E-Mail
F: VoIP
G: Full (WebForum)
H: OSN Messaging (photos, wallposts, activity, etc.)
I: OSN Basic Subscriber Info
J: Videos
. (dot): Indicates multiple types
TOP SECRET//SI//ORCON//NOFORN

XKeyscore

„You could read anyone's email in the world, anybody you've got an email address for. Any website: You can watch traffic to and from it. Any computer that an individual sits at: You can watch it. Any laptop that you're tracking: you can follow it as it moves from place to place throughout the world. It's a one-stop-shop for access to the NSA's information. ... You can tag individuals ... Let's say you work at a major German corporation and I want access to that network, I can track your username on a website on a forum somewhere, I can track your real name, I can track associations with your friends and I can build what's called a fingerprint, which is network activity unique to you, which means anywhere you go in the world, anywhere you try to sort of hide your online presence, your identity.“

https://web.archive.org/web/20140128224439/http://www.ndr.de/ratgeber/netzwelt/snowden277_page-3.html



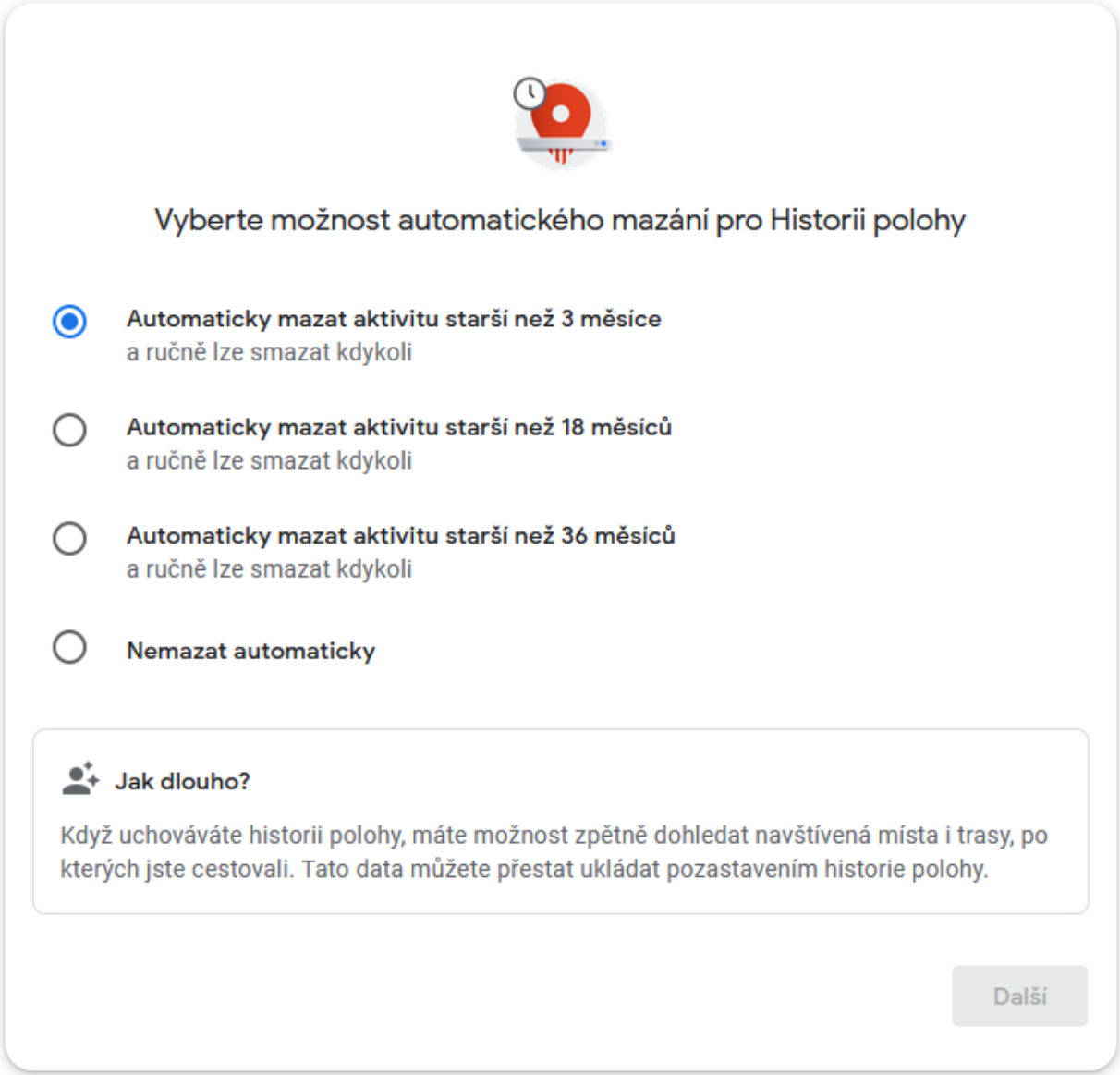
září 2015

1 zajímavé místo

Odpoledne Taneční konzervatoř, Brno, Nejedlého 3

10. 9. 2015

DSA


Vyberte možnost automatického mazání pro Historii polohy
Automaticky mazat aktivitu starší než 3 měsíce
a ručně lze smazat kdykoli
Automaticky mazat aktivitu starší než 18 měsíců
a ručně lze smazat kdykoli
Automaticky mazat aktivitu starší než 36 měsíců
a ručně lze smazat kdykoli
Nemazat automaticky
Jak dlouho?
Když uchováváte historii polohy, máte možnost zpětně dohledat navštívená místa i trasy, po kterých jste cestovali. Tato data můžete přestat ukládat pozastavením historie polohy.
Další

E2E

- *end-to-end šifrování*
- WhatsApp, Signal, Threema – *data v pohybu*

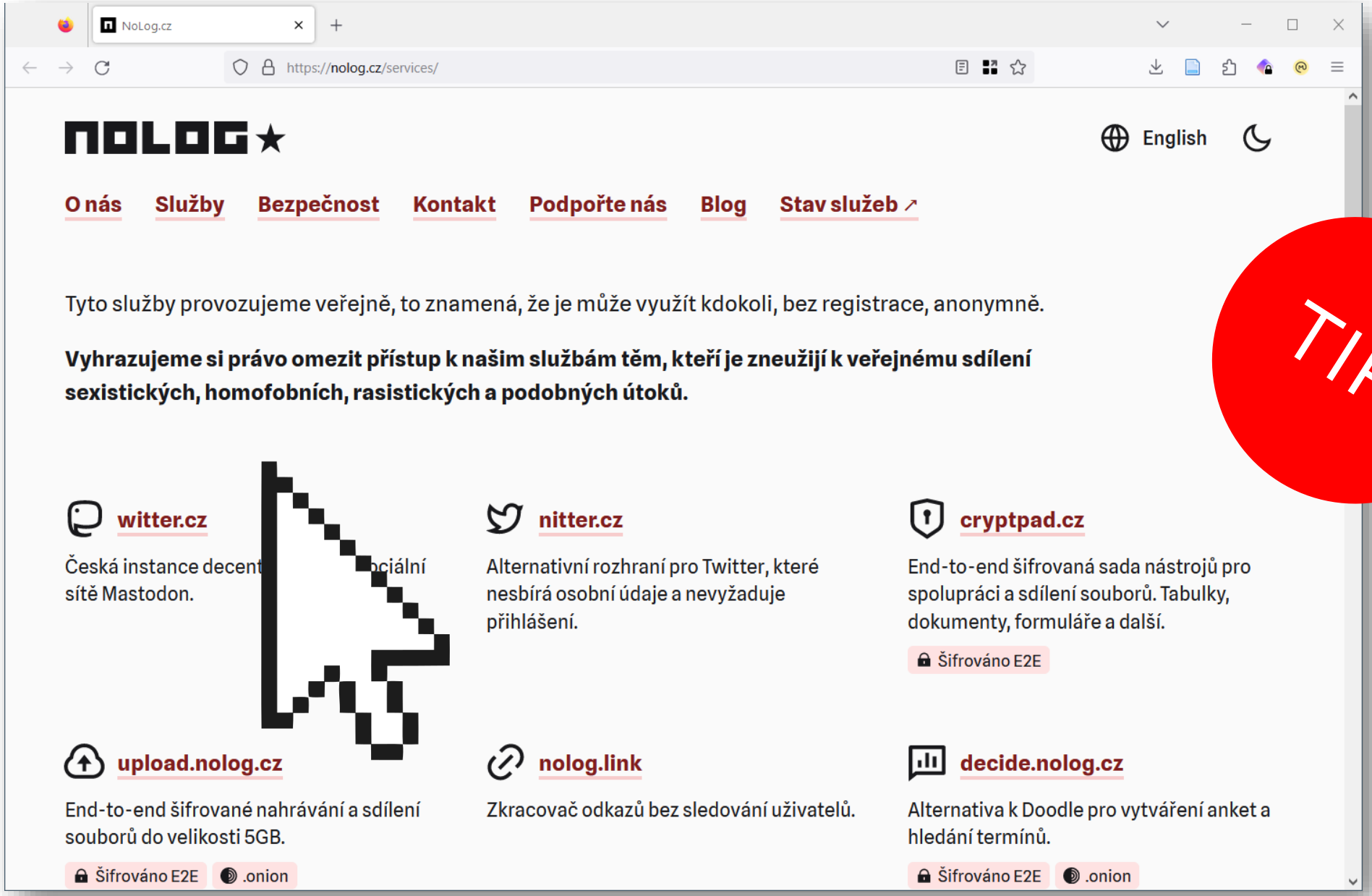
- zadní vrátka a velký boj v EU, UK
- má to jedno slabé místo…

European Court of Human Rights Confirms: Weakening Encryption Violates Fundamental Rights

BY CHRISTOPH SCHMON | MARCH 5, 2024

In a milestone judgment—Podchasov v. Russia—the European Court of Human Rights (ECtHR) has ruled that weakening of encryption can lead to general and indiscriminate surveillance of the communications of *all* users and violates the human right to privacy.

In 2017, the landscape of digital communication in Russia faced a pivotal moment when the government required Telegram Messenger LLP and other "internet communication" providers to store all communication data—and content—for specified durations. These providers were also required to supply

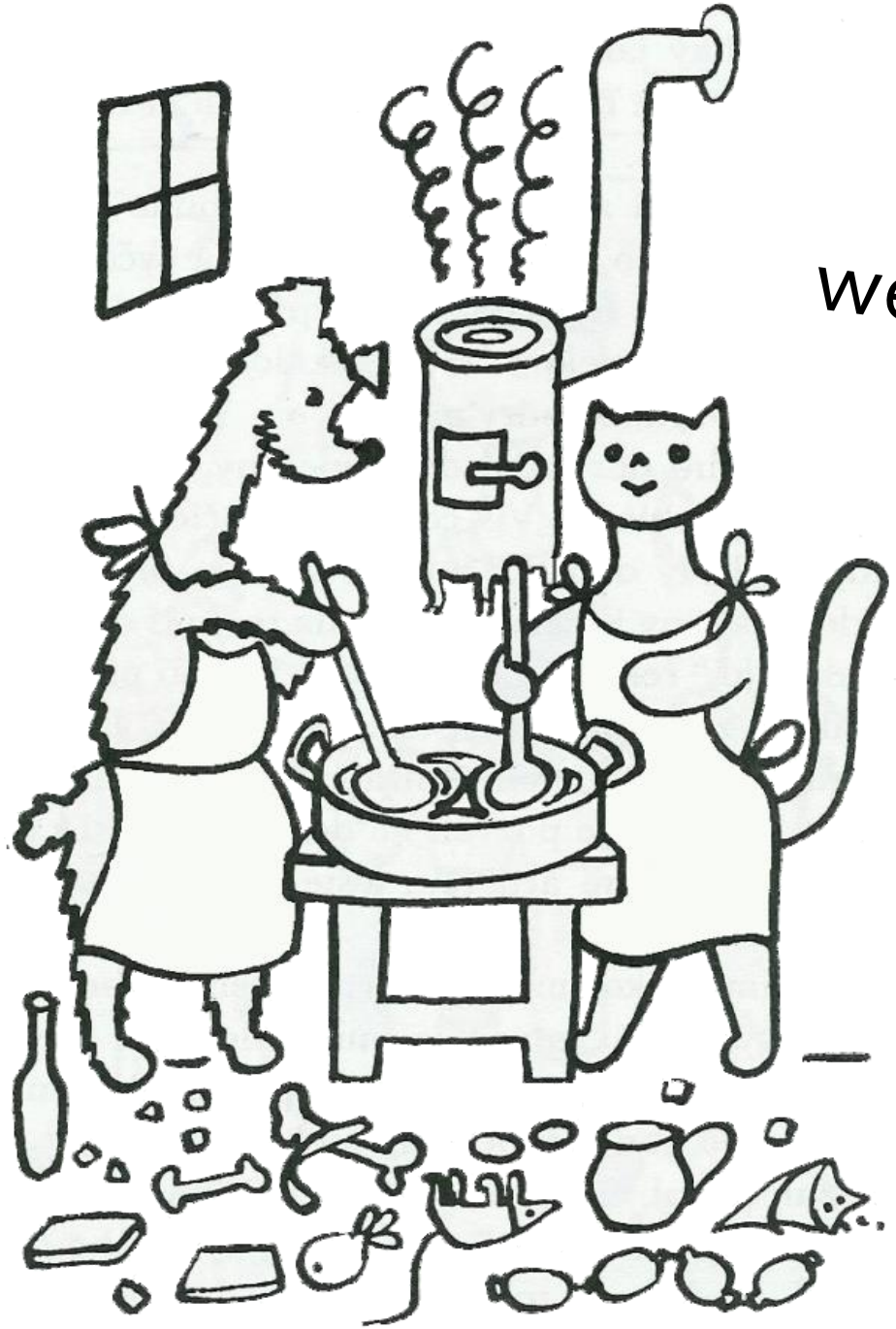

NoLog.cz
https://nolog.cz/services/
NOLOG
English
O nás
Služby
Bezpečnost
Kontakt
Podpořte nás
Blog
Stav služeb ↗
Tyto služby provozujeme veřejně, to znamená, že je může využít kdokoli, bez registrace, anonymně.
Vyhrazujeme si právo omezit přístup k našim službám těm, kteří je zneužijí k veřejnému sdílení sexistických, homofobních, rasistických a podobných útoků.
witter.cz
Česká instance decent
nciální
sítě Mastodon.
nitter.cz
Alternativní rozhraní pro Twitter, které nesbírá osobní údaje a nevyžaduje přihlášení.
cryptpad.cz
End-to-end šifrovaná sada nástrojů pro spolupráci a sdílení souborů. Tabulky, dokumenty, formuláře a další.
Šifrováno E2E
upload.nolog.cz
End-to-end šifrované nahrávání a sdílení souborů do velikosti 5GB.
Šifrováno E2E
.onion
nolog.link
Zkracovač odkazů bez sledování uživatelů.
decide.nolog.cz
Alternativa k Doodle pro vytváření anket a hledání termínů.
Šifrováno E2E
.onion
TIP!

wearables

IoT

telefony

EXIF



Není to jen o počítači...

Každé nové zařízení zapadne do ekosystému.

- mobil jako vstupní brána do vašeho života
- mobil jako další zdroj dat – *všudypřítomný*
- anonymita? – *burner phone*
- IMSI CATCHER – Agáta

GSM

Není to jen o počítači...

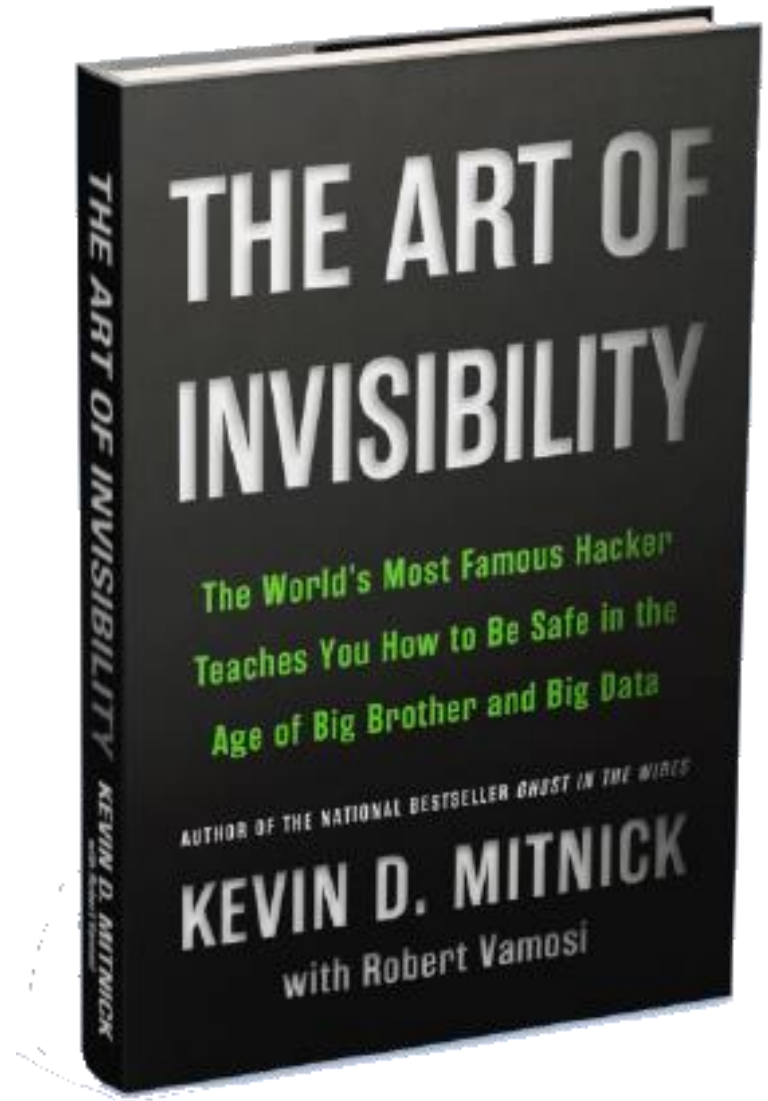
- IoT – internet věcí
- IoT jako zdroj dat - *Shodan*

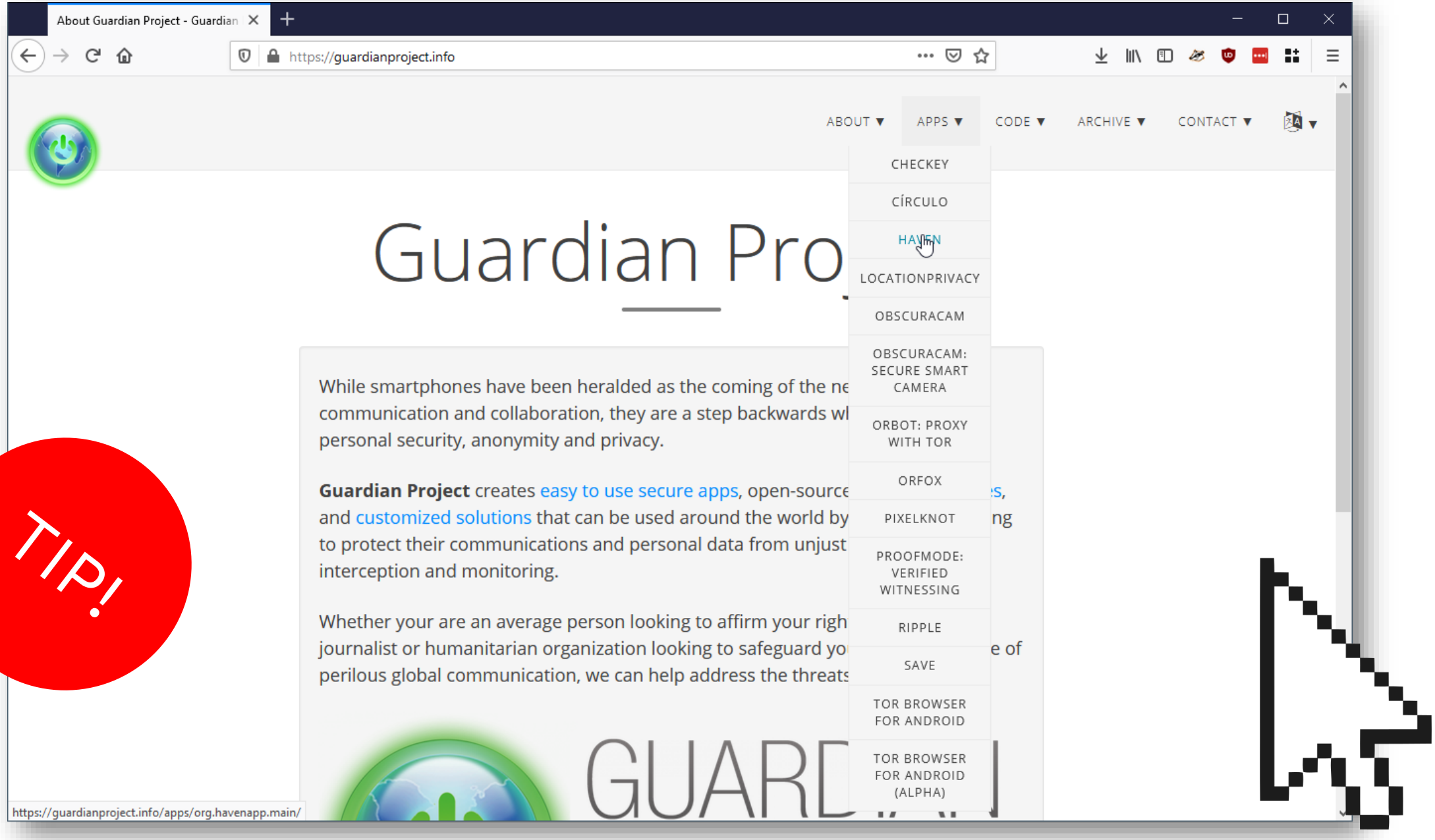
- wearables
- nositelné technologie
- *quantified self*

- IVA - Alexa, Cortana a podobné...
- bezpečnostní problémy

- síťový HW, routery atp.

- fotoaparáty - EXIF informace
- geolokace


THE ART OF INVISIBILITY
KEVIN D. MITNICK
THE ART OF INVISIBILITY
The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data
AUTHOR OF THE NATIONAL BESTSELLER GHOST IN THE WIRES
KEVIN D. MITNICK
with Robert Vamosi


About Guardian Project - Guardian
https://guardianproject.info
ABOUT
APPS
CODE
ARCHIVE
CONTACT
CHECKEY
CÍRCULO
HAVEN
LOCATIONPRIVACY
OBSCURACAM
OBSCURACAM: SECURE SMART CAMERA
ORBOT: PROXY WITH TOR
ORFOX
PIXELKNOT
PROOFMODE: VERIFIED WITNESSING
RIPPLE
SAVE
TOR BROWSER FOR ANDROID
TOR BROWSER FOR ANDROID (ALPHA)
Guardian Pro
While smartphones have been heralded as the coming of the ne
communication and collaboration, they are a step backwards wl
personal security, anonymity and privacy.
Guardian Project creates easy to use secure apps, open-source
and customized solutions that can be used around the world by
to protect their communications and personal data from unjust
interception and monitoring.
Whether your are an average person looking to affirm your righ
journalist or humanitarian organization looking to safeguard yo
perilous global communication, we can help address the threats
https://guardianproject.info/apps/org.havenapp.main/

TIP!

čím více bezpečí a anonymity,
tím více nepohodlí