Nástroje a možnosti internetu

Internet jako nástroj sledování

22. 10. 2021

Fu*kUp ~~Night~~:
selhali jste někdy
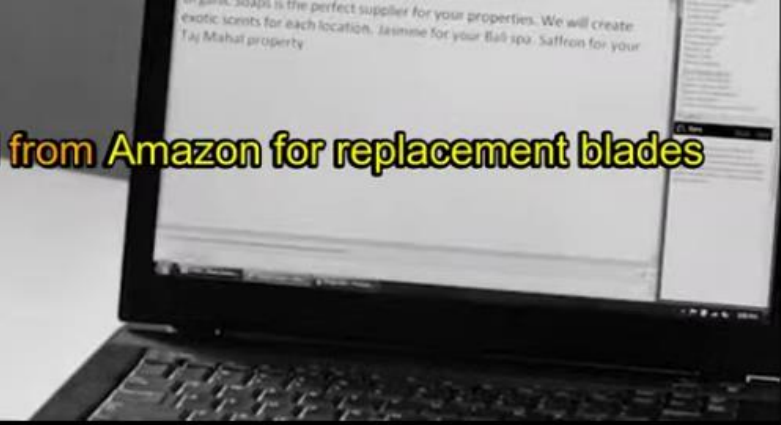při ochraně své
kyberbezpečnosti?

komercionalizace Internetu

data-driven svět

soukromí a anonymita

Měli jste někdy pocit,
že jste na Internetu
sledováni?

from Amazon for replacement blades

I happened to be on Facebook at

and starts scrolling through my Insta
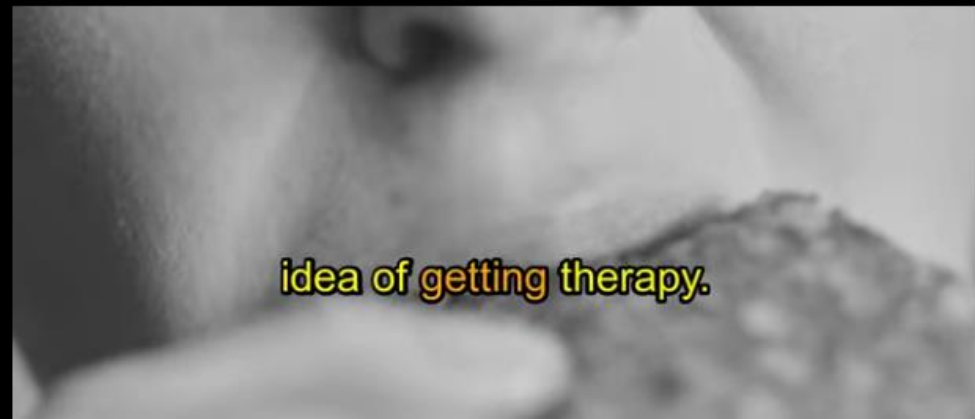
ads a few days before I get

One day was talking with my friends

just pictures.

is Hammermill Color Copy 28lb,

idea of getting therapy.

for pregnancy tests and dating sit

Marketing Technology Landscape
The Martech 5000

chiefmartec.com — April 2020

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
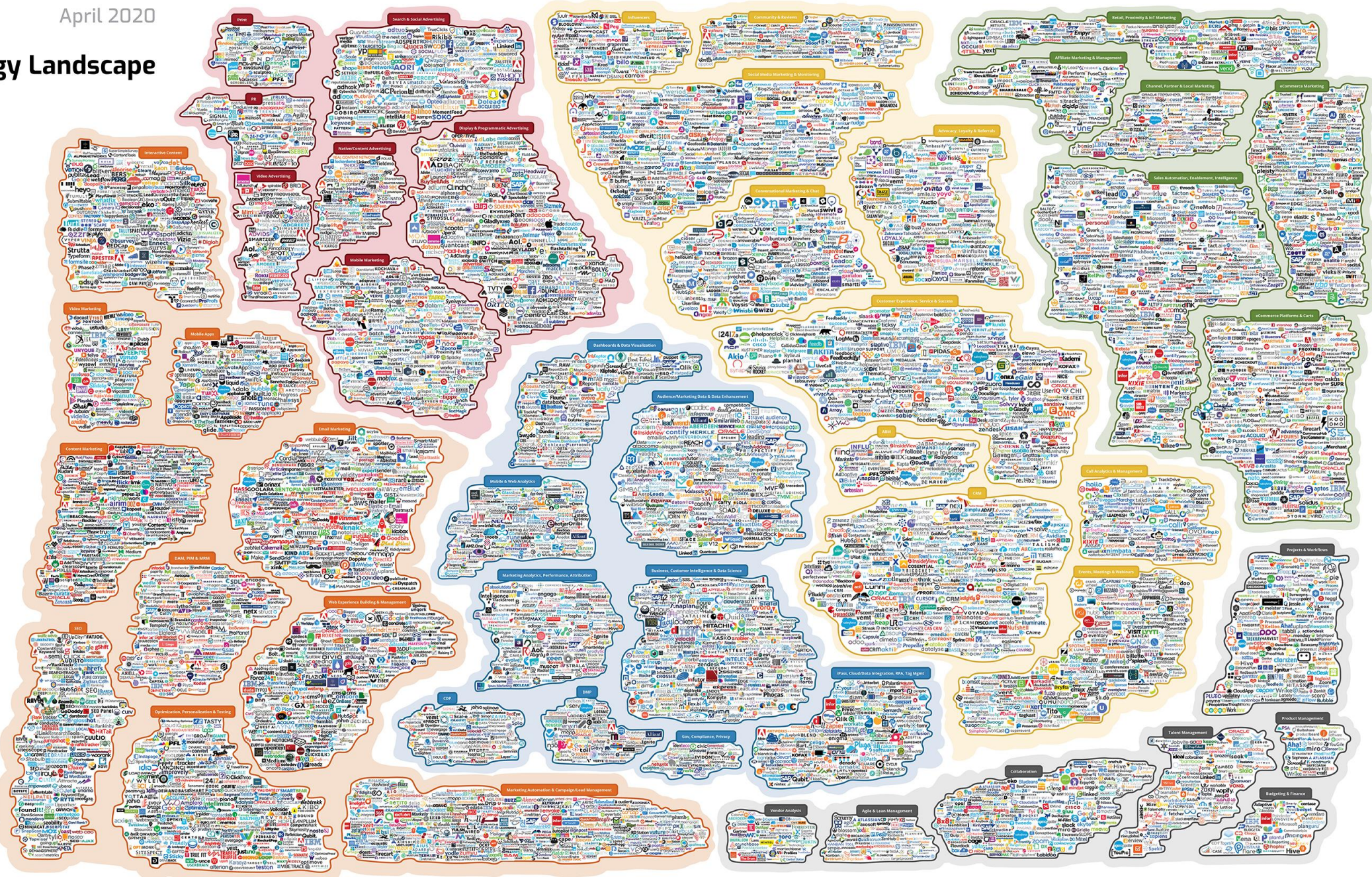2018 — 6,829 solutions
2017 — 5,381 solutions
2016 — 3,874 solutions
2015 — 1,876 solutions
2014 — 947 solutions

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

Search jobs   Sign in   Search   International edition

The Guardian

News   Opinion   Sport   Culture   Lifestyle   More ⌄

Media & Tech Network

Jon Card

Mon 22 Jun 2015 12.00 BST

f t ✉   45 0

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

▲ 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.

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

Řešíte **aktivně** své soukromí na Internetu?

Časté argumenty

„Když nemáš co skrývat…“

Časté argumenty

„Když nemáš co skrývat...“

- Jeremy Bentham - *Panopticon*
- vězení mysli
- *disident či novinář = špatný člověk?*
- společenské změny

Časté argumenty

„Soukromí už není sociální norma..."

„Nelze se tomu vyhnout, tak nemá cenu to řešit..."

Michal Kosinski:
• soukromí je mrtvé
• 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. "

Časté argumenty

„Nepoužívám *to*, tak to nemusím řešit…"

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

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

Časté argumenty

„Personalizovaná reklama je OK..."

„Nějak se ty služby platit musí."

- *kapitalismus dohledu*
- Cambridge Analytica
- [technologie není apolitická](#)
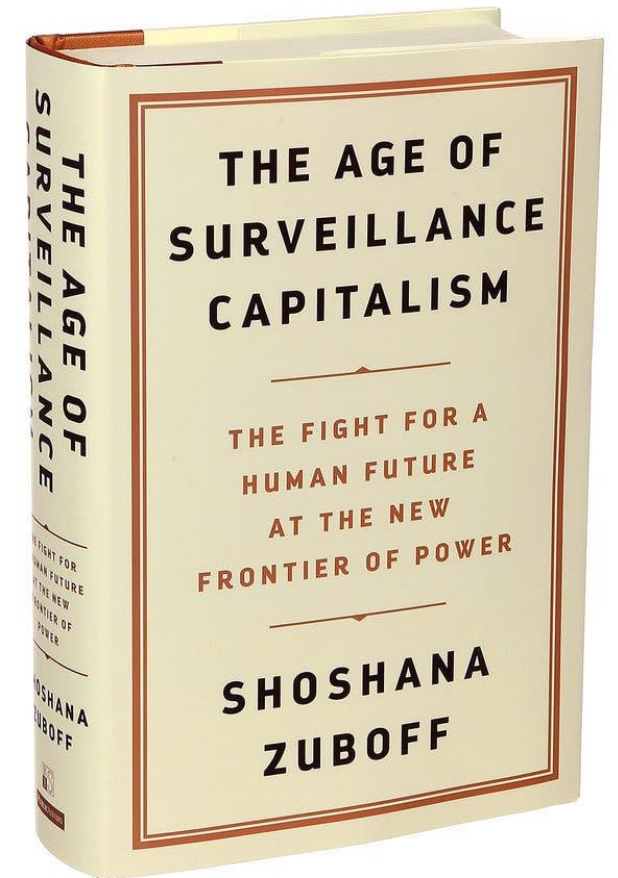
Časté argumenty

„Když to pomůže zastavit špatné lidi…"

• soukromí vs. bezpečnost
• evaluace efektivity

Přístupy k ochraně dat

- 27 % dospělých uživatelů využívalo VPN
- 57 % lidí se bálo, že jejich data nejsou v bezpečí
- 14 % uživatelů bylo OK se sdílením dat společnostmi
- 1 ze 4 četl [ToS](#) před přihlášením do služby

„Despite much concern about the security and privacy of data, many are unsure what to do to better protect their data [...] the behaviour of many Europeans is not reflected by their actions towards data protection."

bezpečnostní gramotnost

Do you know what private browsing is?

No, 45%

Yes, 55%

2012

No, 38%

Yes, 61%
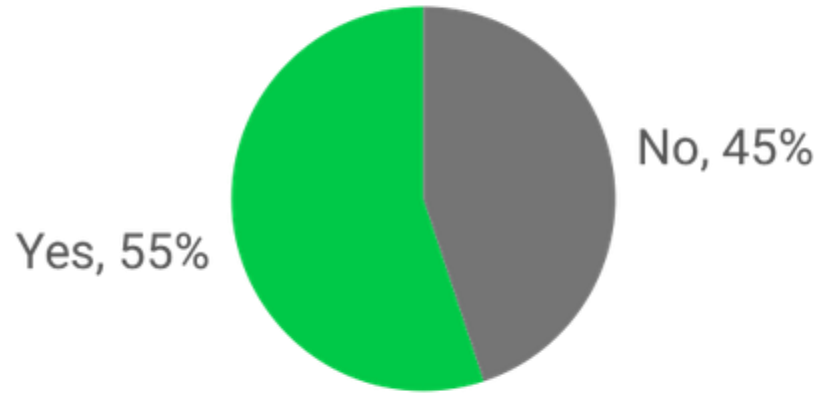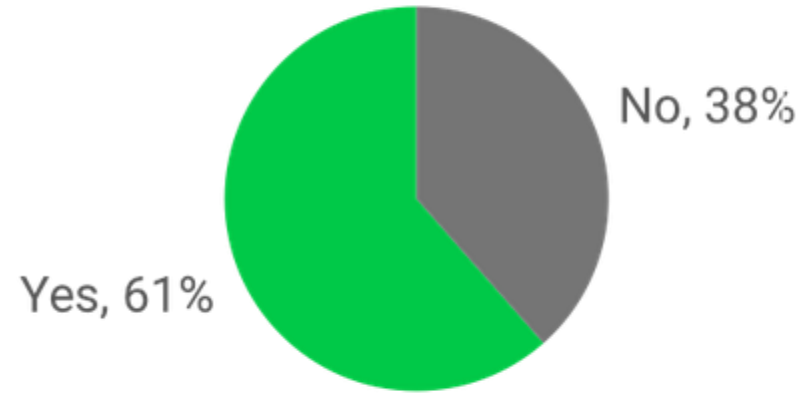
2017

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%
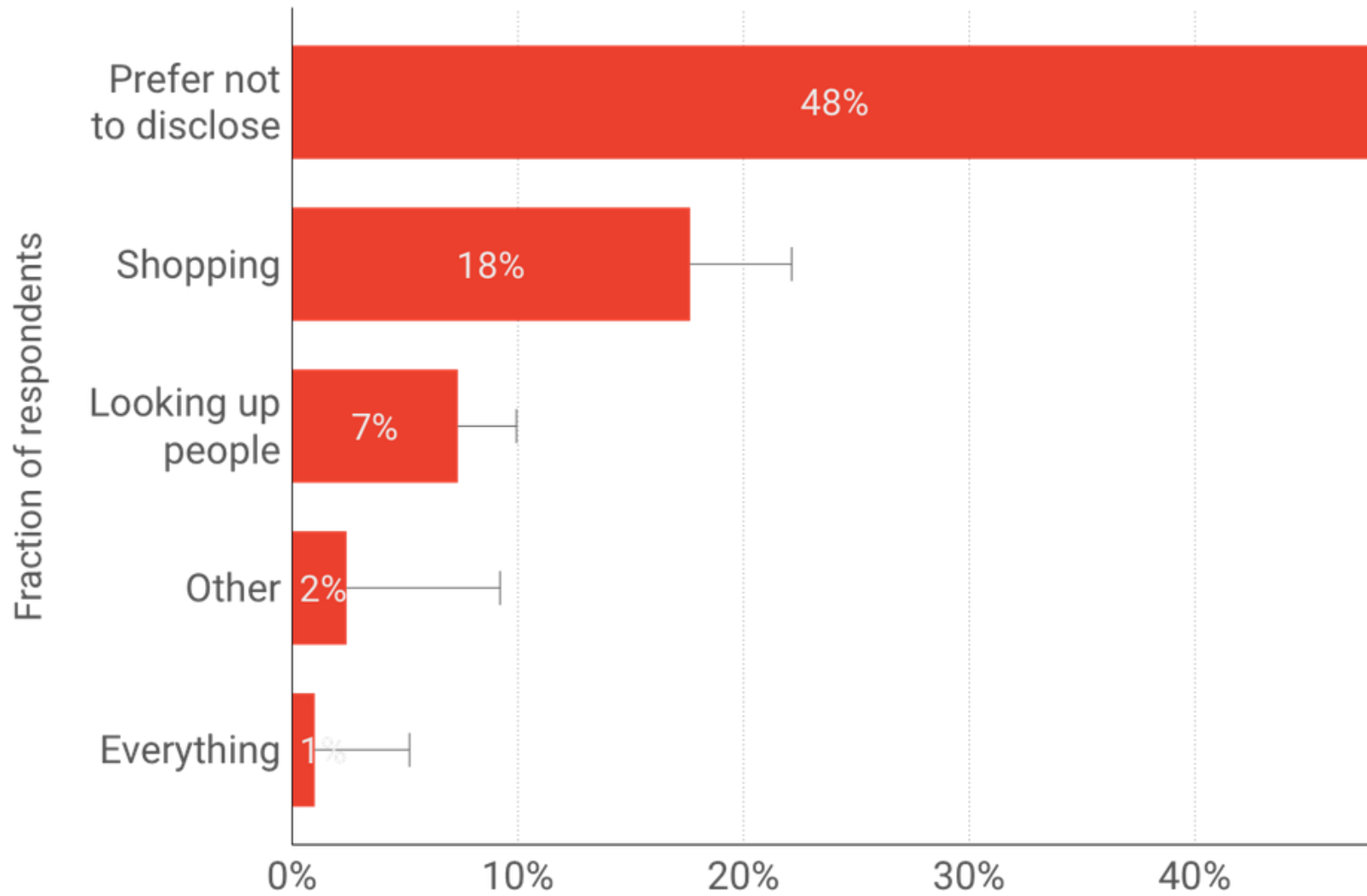
Anonymní režim prohlížeče používám, abych se ochránil/a před sledováním ze strany...

You use private browsing to hide from...

Category	Percentage
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%
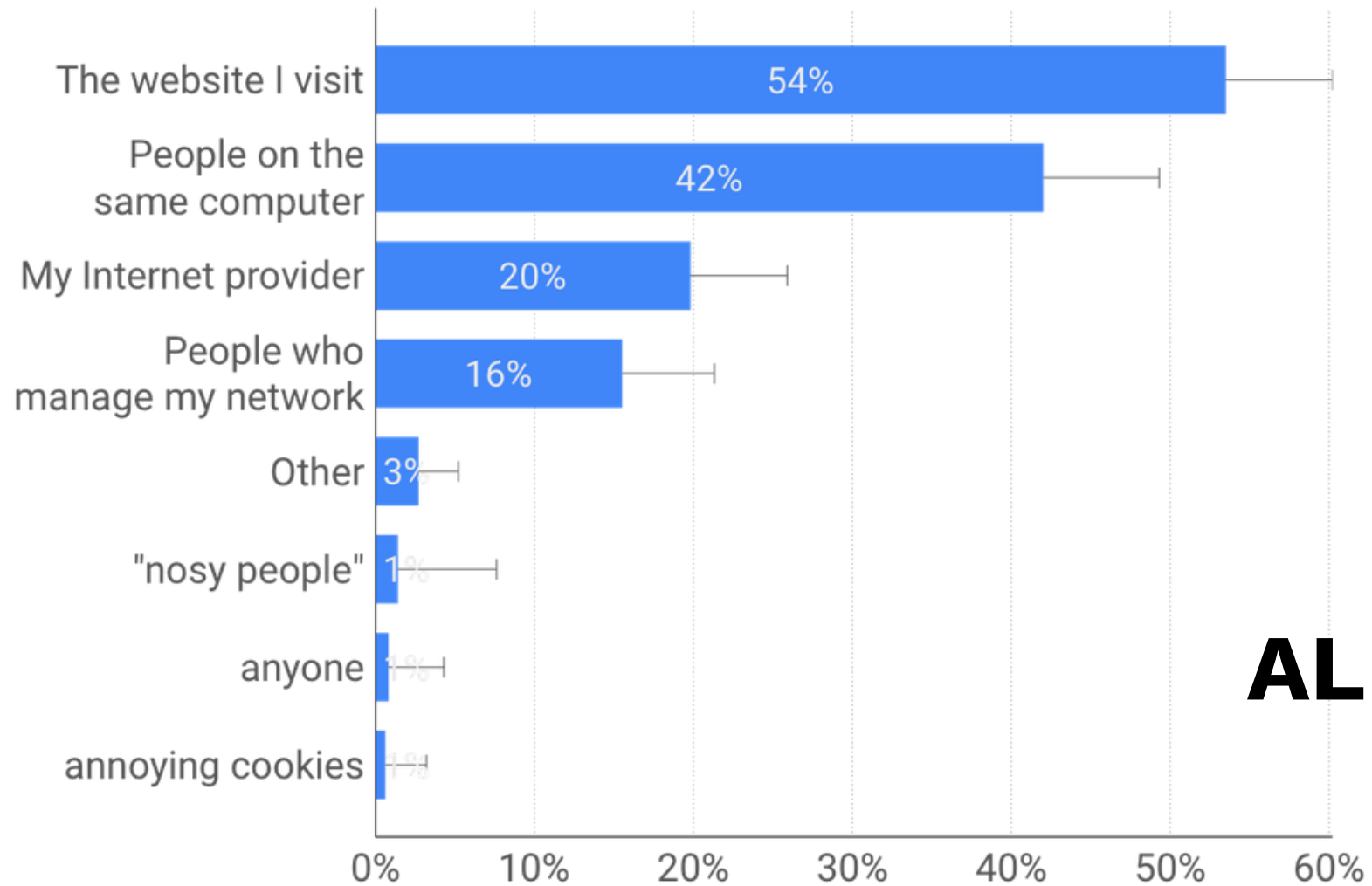
ALE...!

profilování & targeting

Profilování

- *Michal Kosinski*
- modelování vlastností

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

📄 HTML

Published
2009-09-25

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

More Citation Formats

Issue
Volume 14, Number 10 -
2009

Section
Articles

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.

Authors retain copyright t
published in *First Monday*.
footer of each article for d

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-

Datové zplodiny

- *data exhaust*
- NPI vs. **PII**
- digitální stopa

- *aktivní a pasivní digitální stopa*
- *nepřímá digitální stopa (skrze sociální propojení)*

Jak můžeme na Internetu **jednoznačně** identifikovat uživatele? 👋
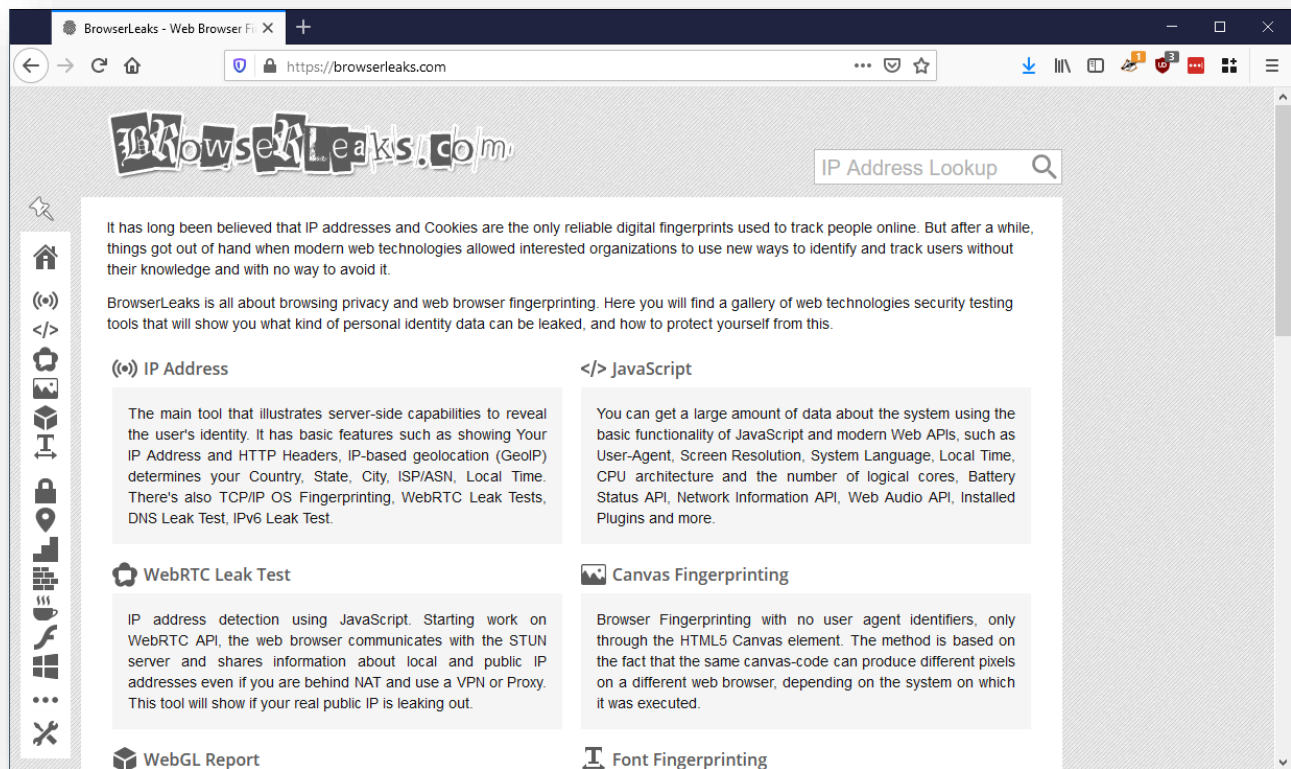
Identifikace

- *datoví paraziti*
- *retargeting*

- cookies
- sledovací skripty
- *FB Pixel*
- fingerprinting

cookies

sledovací skripty

browser & canvas fingerprinting

BrowserLeaks - Web Browser Fi... +

https://browserleaks.com

BrowseRLeaks.com

IP Address Lookup

It has long been believed that IP addresses and Cookies are the only reliable digital fingerprints used to track people online. But after a while, things got out of hand when modern web technologies allowed interested organizations to use new ways to identify and track users without their knowledge and with no way to avoid it.

BrowserLeaks is all about browsing privacy and web browser fingerprinting. Here you will find a gallery of web technologies security testing tools that will show you what kind of personal identity data can be leaked, and how to protect yourself from this.

IP Address

The main tool that illustrates server-side capabilities to reveal the user's identity. It has basic features such as showing Your IP Address and HTTP Headers, IP-based geolocation (GeoIP) determines your Country, State, City, ISP/ASN, Local Time. There's also TCP/IP OS Fingerprinting, WebRTC Leak Tests, DNS Leak Test, IPv6 Leak Test.

JavaScript

You can get a large amount of data about the system using the basic functionality of JavaScript and modern Web APIs, such as User-Agent, Screen Resolution, System Language, Local Time, CPU architecture and the number of logical cores, Battery Status API, Network Information API, Web Audio API, Installed Plugins and more.

WebRTC Leak Test

IP address detection using JavaScript. Starting work on WebRTC API, the web browser communicates with the STUN server and shares information about local and public IP addresses even if you are behind NAT and use a VPN or Proxy. This tool will show if your real public IP is leaking out.

Canvas Fingerprinting

Browser Fingerprinting with no user agent identifiers, only through the HTML5 Canvas element. The method is based on the fact that the same canvas-code can produce different pixels on a different web browser, depending on the system on which it was executed.

WebGL Report

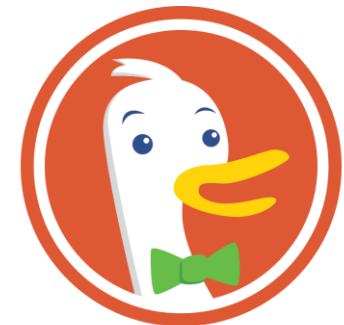### Font Fingerprinting

COVER YOUR TRACKS

„Anonymní" prohlížeče

- prohlížeče se striktním přístupem ke sledování
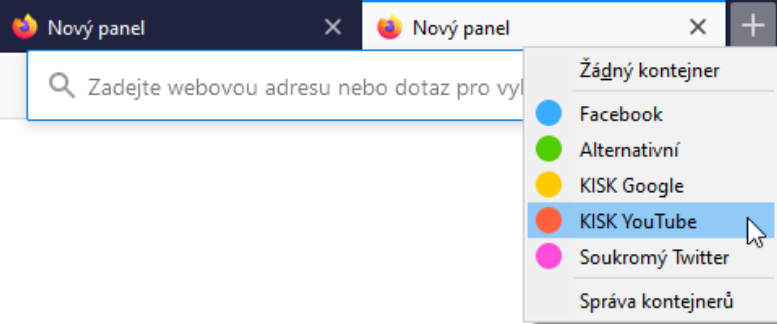- většina blokací přímo zabudována
- EPIC Browser
- Brave

„Anonymní" vyhledávání

- vyhledávače s odlišným modelem monetizace
- nesbírají data o uživatelích
- neprodávají reklamní prostor
- *za jakou cenu?*

- DuckDuckGo
- Další anonymní vyhledávače

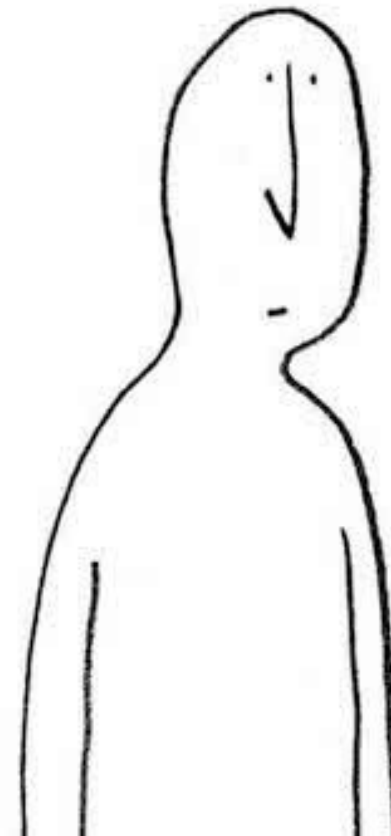# Jak to mám já?

- Firefox – *implementované nástroje*
- blokování reklamy (*uBlock Origin)*
- blokování skriptů *(Privacy Badger)*
- [Firefox Containers](#)

Web týdne

https://nolog.cz/services/

🌐 English

NoLog.cz IT kolektiv

O nás Služby Bezpečnost Kontakt Podpořte nás Status Blog

Služby

Většinu služeb provozujeme ve spolupráci s konkrétní skupinou nebo organizací v rámci uzavřeného kolektivu.

Dokážeme poskytnout nástroje pro vnitřní komunikaci, hosting webů, e-mailů, sdílené úložiště souborů i celé virtuální servery.

Pokud se shodujete s našimi hodnotami a máte o naše služby zájem, napište nám.

Některé služby provozujeme veřejně, to znamená že je může využít kdokoli, bez registrace, anonymně.

👁 - Služba **nevyužívá** E2E šifrování.
🔒 - Služba **využívá** E2E šifrování.

pad.nolog.cz 👁
Pad.nolog.cz umožňuje tvořit a editovat textový dokument ve více lidech. Vhodné pro tvorbu tiskových prohlášení, checklistů při organizování demonstrací apod.

upload.nolog.cz 🔒
Upload.nolog.cz slouží k nahrávání a sdílení souborů (až 2GB).

decide.nolog.cz 🔒
Decide.nolog.cz umožňuje tvorbu anket a pomůže vám vybrat vhodné datum schůzky.

Služby / Services

- pad.nolog.cz
- upload.nolog.cz
- wiki.nolog.cz
- decide.nolog.cz
- paste.nolog.cz
- ticker.nolog.cz
- calc.nolog.cz
- call.nolog.cz
- bridge.nolog.cz
- unshort.nolog.cz
- acab.link/nolog.link