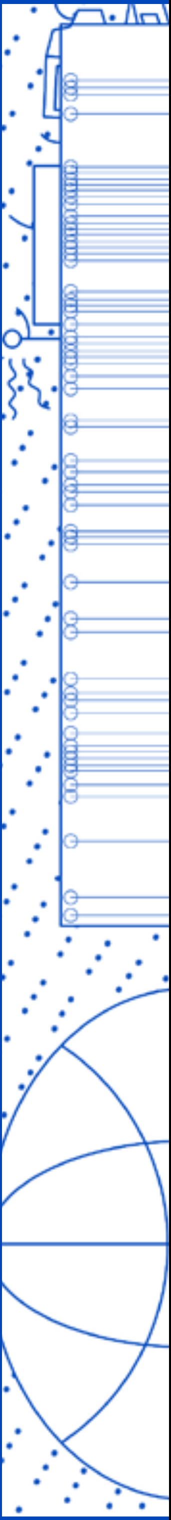


Meatspace Press

EATEN BY THE INTERNET

EDITED BY
CORINNE CATH

With contributions by

Meredith Whittaker
Yung Au
Shivan Kaul Sahib
Michael Veale
Britt Paris
Fieke Jansen
Suzanne van Geuns
Gurshabad Grover

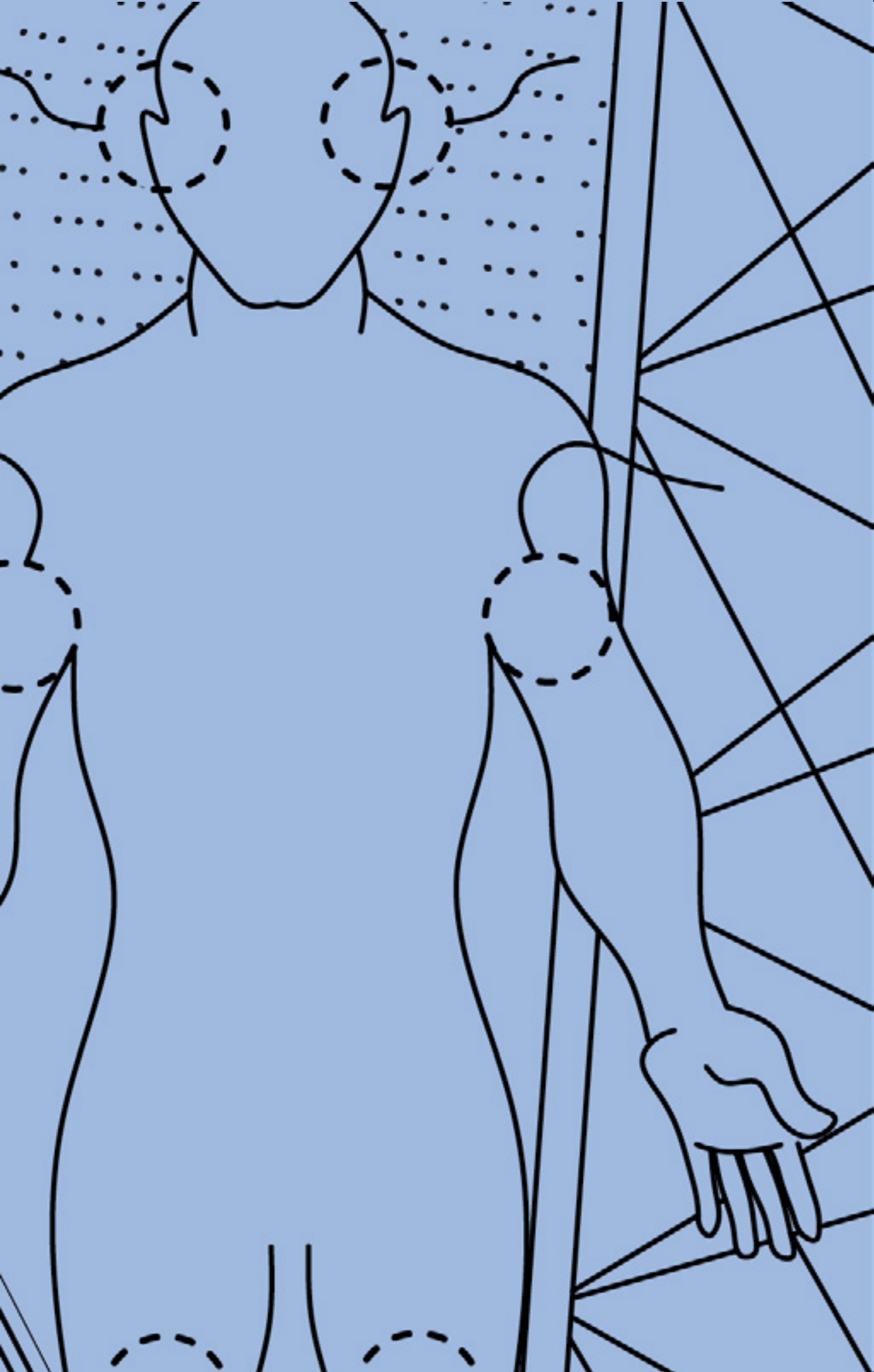
Ksenia Ermoshina
Francesca Musiani
Mallory Knodel
Niels ten Oever
Maxigas
Ashwin Mathew
Mehwish Ansari
Jenna Ruddock
Joan Donovan

Eaten by the Internet

Edited by: Corinne Cath
Publisher: Meatspace Press (2023)
Place of publication: Manchester, United Kingdom
Weblink: meatspacepress.com
Design: Carlos Romo-Melgar and John Philip Sage
Commissioning editors: Mark Graham and Joe Shaw
Managing editor: David Sutcliffe
Copy editor: Suzanne van Geuns
Format: Paperback and pdf
Length: 128 pages
Language: English
Product code: MSP231001
ISBN (paperback): 9781913824044
ISBN (pdf, e-book): 978191382405
DOI: https://doi.org/10.58704/dmnx-1r61
License: Creative Commons BY-NC-SA

Contributors (alphabetically): Mehwish Ansari, Yung Au, Corinne Cath, Joan Donovan, Ksenia Ermoshina, Suzanne van Geuns, Gurshabad Grover, Fieke Jansen, Mallory Knodel, Ashwin Mathew, Maxigas, Francesca Musiani, Niels ten Oever, Britt Paris, Jenna Ruddock, Shivan Kaul Sahib, Michael Veale, and Meredith Whittaker.

The publisher has endeavoured to ensure that any URL for external websites referred to in this book are correct and active at the time of going to press. However, the publisher has no responsibility for the websites and can make no guarantee that these links remain live or that the content is, or will remain, appropriate for all audiences.

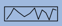


59 Confidentiality washing in online advertising

60 Michael Veale

Michael Veale is associate professor in the Faculty of Laws, UCL. He researches tensions between emerging technologies, their societal impacts, and their legal characteristics.

61 Keywords: big tech, confidentiality, encryption, online ad economy, privacy

62 Online advertising has long been a privacy
shitshow. Whenever apps or websites try to
show an ad to someone, they send data about
that viewer to hundreds of would-be bidders,
who act for big brands looking for the right
audiences. These bidders in turn send the data
to hundreds more data brokers, to learn as
much as possible about the viewer—all just to
work out a reasonable maximum bid for their
attention. This arrangement has long been deeply
illegal, but its complexity and opacity has left
regulators paralysed . Thanks to new(ish)
63 laws, regulators creaking into action, and tracker
blockers in browsers, we may see the end of this
invasive practice.

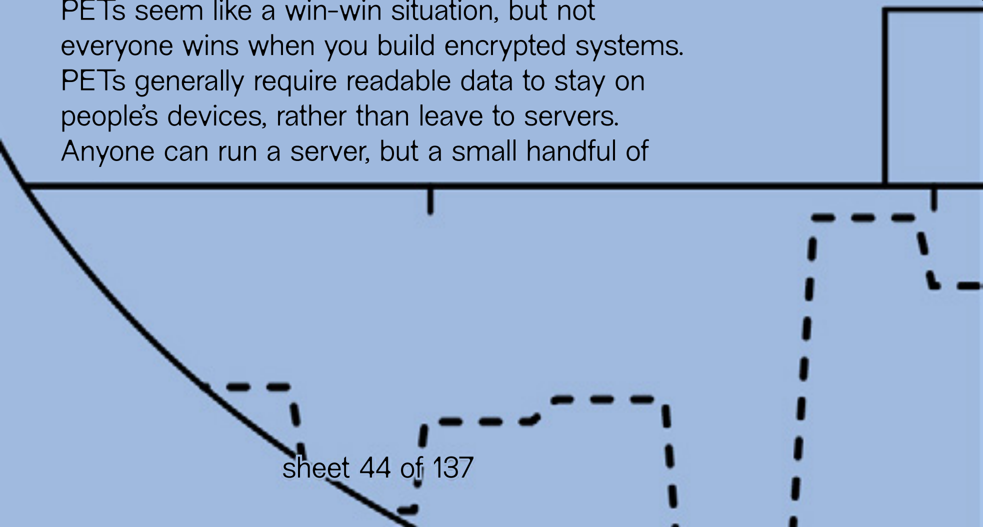
It would, however, be naïve to think this will be the end of online tracking. Advertising has left so many marks on internet economics and internet infrastructures that it can be a struggle to imagine alternatives. In this piece, we look at the power struggles emerging around these replacements, as well as examining what exactly these proposals improve upon, and which aspects might instead be spin, distraction, or mirage.

Proposed replacements centre on a bundle of intriguing tools called 'privacy-enhancing technologies', or PETs. To use PETs, first you think of a task you want to do that typically relies on a lot of people moving a lot of data—like browsing the Web, analysing medical records from many clinics, or communicating with a group of people—and then build a set of technologies that lets you do it while only collecting or disclosing the minimum of information to untrusted people . The results can be surprising and counterintuitive. In the case of online advertising, imagine deeply targeted ads, but chosen and delivered without personal data ever leaving your device in a form others can pry upon. PETs excite people precisely because it appears that society can both have its cake and eat it: keeping the business model, while protecting privacy.

64

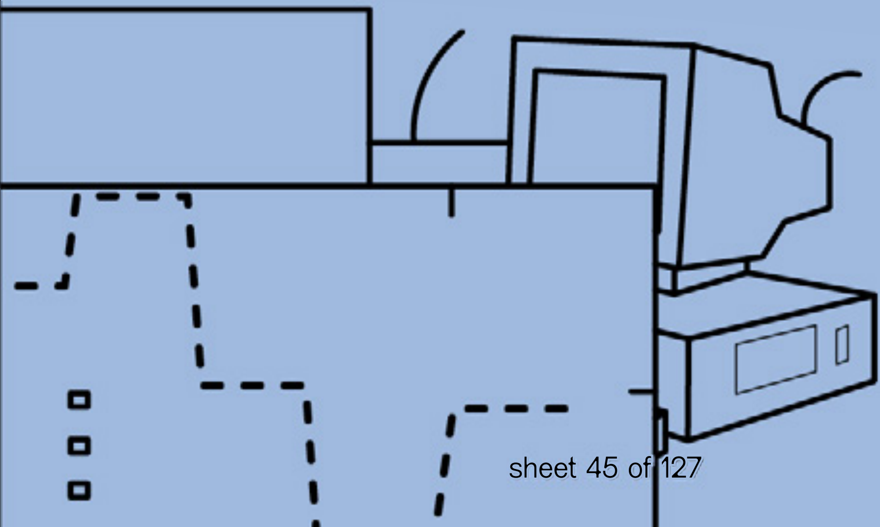
PRIVACY IS POWER—BUT NOT FOR YOU

PETs seem like a win-win situation, but not everyone wins when you build encrypted systems. PETs generally require readable data to stay on people's devices, rather than leave to servers. Anyone can run a server, but a small handful of



firms have real strangleholds on the large-scale computational infrastructures needed for PETs, including for what devices like phones can do. These include operating system providers—like Apple and Google—browser providers—like Apple and Google—and app store providers like—yes!—Apple and Google. In contrast, smaller adtech firms are not well positioned to benefit from a change to PETs. Such adtech firms' infrastructure is only skin-deep; it cannot do complex computing, as is required for most PETs to function.

PETs even make a company like Meta feel vulnerable. It controls significant parts of the top of the technology stack, such as apps, and even some of the bottom, like undersea cables but lacks much of the middle. Meta has no major operating system, browser, or app store. This leaves the firm reliant on decisions made by Apple and Google. When Apple forced an opt-in function for a certain type of tracking across apps in mid-2021, Meta reported a significant hit to its revenue, as this limited the firm's ability to gather data on which
65 apps people use and how. The firm is undoubtedly worried more moves are yet to come .



CONFIDENTIALITY WASHING

Data giant Meta's PET anxieties show the power PETs can give infrastructure providers but will probably not stir huge sympathies in the reader. Yet there are other reasons to keep a critical eye over the specific way PETs are developing. If PETs are a solution to adtech's woes, what is the problem? Proponents would have you believe the problem is a lack of confidentiality—the ability to protect data about you from being looked at by others. This is certainly a problem. The leaky adtech stack is regularly abused in diverse ways, from outing individuals' sexual orientation to being piggybacked upon by intelligence services and the military to identify targets. But what problems remain 66
even when confidentiality is secured?

We can imagine an on-device, targeting system which transfers no data off-device, yet bases ads on comprehensive browsing data or deeply personal health data from wearables. This may be confidential, but is it private? Even if a tech company employee cannot read your Web history, your device itself is trampling over personal boundaries in ways you may not be able to stop or control. Even if you could turn these settings off, we can imagine a company making access to free services, like cloud storage or online subscriptions, conditional on confidential analysis and targeting. Because this data is kept confidential, there is even a potential perverse outcome where companies try to use more sensitive data than before as part of their business models, arguing that it's fair game if not transmitted or centralised. This would be a world of confidentiality washing, where devices and their corporate manufacturers, instead of the servers of platform companies, are betraying, profiling, and manipulating users—under the guise of confidentiality [67]. Is that much of an improvement?

ENCRYPT ALL THE THINGS?

This situation places civil society organisations in a bind. Since Snowden, they have successfully rallied companies and the public behind encrypting communications, limiting some forms of state surveillance. But encryption technologies have moved on, and they can now more effectively encrypt analysis and computation as well. This is a much more open design space, where businesses can design complex PETs to advantage them to the detriment of their competitors [68].

The debates about the politics of encryption are changing. It is no longer about encrypting a chat or a call. In many ways, it is more like encrypting a clinical trial, a company's tax payments, or a government policy. Activists defend encryption by talking about freedom to decide how we communicate—the means—regardless of what messages contain. Critics respond by reframing it as about the ends of certain communication, typically highlighting child abuse and serious crime. But encryption is no longer just about communication or expression. The ends that can be encrypted now include large-scale data analysis or entire internet business models. This quickly, and confusingly, blurs personal privacy and corporate opacity.

In an already highly technical domain, the thought of further complicating messaging will make civil society queasy. But unless they start to navigate these turbulent waters, they risk tying the legitimate protection of encrypted expression to the questionable legitimacy of any business or surveillance practice that can be confidentiality-washed using PETs. As encryption goes from a narrow-purposed set of tools to an infrastructure supporting broad, open-ended computing systems, we cannot afford to see it as simply 'good' or 'bad'. Instead, we must ask the questions we should always be asking of all powerful systems: Who put them there? Who do they functionally benefit? And most importantly—how can we negotiate, or if necessary, refuse and reject them?

Notes:

[63] Veale, M. and Borgesius, F.Z. 2022. Adtech and Real-Time Bidding under European Data Protection Law. *German Law Journal* 23: 226–256 doi.org/jphn; Veale, M., Nouwens, M. and Santos, C. 2022. Impossible Asks: Can the Transparency and Consent Framework Ever Authorise Real-Time Bidding After the Belgian DPA Decision? *Technology and Regulation* 2022, 12–22. doi.org/gpgcfb

[64] Gürses, S., Troncoso, C. and Diaz, C. 2015. Engineering Privacy by Design Reloaded. Amsterdam Privacy Conference 2015. https://perma.cc/C77G-5EP9

[65] Meta has thus been active within internet standardisation bodies, trying to shift the narrative towards PETs which rely more on servers—so far with limited success. See archived Google Slides at https://perma.cc/LBW3-TB64; archived Google Doc at https://perma.cc/28UN-F8VB; Veale, M. 2022. Future of online advertising: Adtech's new clothes might redefine privacy more than they reform profiling. netzpolitik.org. https://perma.cc/EYC4-66H6

[66] Modderkolk, H. 2014. Lees hier hoe de Britse geheime dienst GCHQ Belgacom aanviel. NRC. https://www.nrc.nl/nieuws/2014/12/13/verantwoording-en-documenten-a1420301; Soltani, A., Peterson, A. and Gellman, B. 2013. NSA uses Google cookies to pinpoint targets for hacking. Washington Post. https://www.washingtonpost.com/news/the-switch/wp/2013/12/10/nsa-uses-google-cookies-to-pinpoint-targets-for-hacking/; O'Brien, M., and Bajak, F. 2021. Priest outed via Grindr app highlights rampant data tracking. AP. https://apnews.com/article/technology-europe-business-religion-data-privacy-97334ed1aca5bd363263c92f6de2caa2

[67] See relatedly Berjon, R. 2021. The Fiduciary Duties of User Agents. Pre-print https://doi.org/10/gjw466; Renieris, E. 2021. Why PETs (privacy-enhancing technologies) may not always be our friends. Ada Lovelace Institute. https://perma.cc/E84R-V93V

[68] Rogaway, P. 2015. The Moral Character of Cryptographic Work. Essay accompanying the IACR Distinguished Lecture, AsiaCrypt 2015. https://perma.cc/KV9S-B7LJ

This book makes internet infrastructure visible as a force of political power, which is transforming the social world, from the bottom up—through fifteen chapters contributed by a global set of researchers, activists, and techies. We are living a unique moment: internet technologies are the default infrastructure for society, not just how we communicate but also how we organise our social life, politics, and economy, all the way down to our material environments, like cities. Our world is eaten by the internet. This means that those who control the internet control the bounds of public speech, economic production, social cohesion, and politics, making its infrastructure a core political terrain in the networked age. The book's chapters cover a wide set of topics, spanning from the global politics of content moderation by internet infrastructure to the colonialism inherent in the race to plug the moon, from the harms wrought by blockchain companies in rural America to the particularities of online censorship across Asia. The chapters take on thorny topics, discussing power consolidation in the advertisement and cloud industry, the role of internet infrastructure in the war in Ukraine, and tech's environmental impact—amongst others. In doing so, this book roots contemporary technology debates in the politics of internet infrastructure and urges us to ask how can we ensure our infrastructures sustain us, rather than consume us?

ISBN 978-1-913824-04-4

9 781913 824044

www.meatspacepress.com