SMASHING
MAGAZINE PRINT

Ethics & Privacy

1

Designing For Addiction
by Trine Falbe

This One Weird Trick Tells Us Everything About You
by Laura Kalbag

Advertising Is Not The Problem
by Cennydd Bowles

Published 2019 by Smashing Media AG, Freiburg, Germany.
Cover illustrator: Veerle Pieters
Editors: Rachel Andrew and Owen Gregory
Typesetters: Alex Clarke, Rachel Andrew and Markus Seyfferth
All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopy, recording or any information storage and retrieval system, without prior permission in writing from the publisher.
ISBN: 978-3-945749-79-1

1

CONTENTS

Editor's Note

by Rachel Andrew

6

Designing For Addiction

by Trine Falbe

17

8

Towards Ethics By Default, One Step At A Time

by Vitaly Friedman

28

It's Not About You

by Heather Burns and Morten Rand-Hendriksen

This One Weird Trick Tells Us Everything About You

by Laura Kalbag

35

Advertising Is Not The Problem

by Cennydd Bowles

53

46

Quieting Disquiet

by Stuart Langridge

Editor's Note

WELCOME TO THE VERY FIRST SMASHING MAGAZINE PRINT. This is the pilot issue of our new magazine. Each issue will follow a different theme. We intend the print magazine to cover broader topics that perhaps have more longevity than some of the subjects we cover in the online magazine – the big picture issues that we all deal with as people who work on the web. We kick off with an issue covering ethics, privacy, and security, because they reach into all our lives, from our personal use of the internet, through to the applications we develop.

Rather than ask the authors of this first issue to write on a very specific topic, I asked them to tell me what they felt they could contribute to a collection of thinking on the subjects of ethics, privacy, and security. What follows is a group of essays which sit very well together, yet tackle different aspects of the matters at hand. You may not agree with all of them, but I hope they make you think.

Editing a print publication isn't something I had in mind when I became editor-in-chief of Smashing Magazine. It has been a very different sort of challenge selecting the pieces for this first publication.

Along with the themed essays, we have included some little insights into the world of Smashing Magazine, pieces about our conferences, books, and membership. Smashing Magazine is brought to you by a tiny team of people who care. They care about Smashing, and care about the people who read the magazine, join as members, and come to the conferences. They care a lot about the web. I hope that shines through in everything we do.

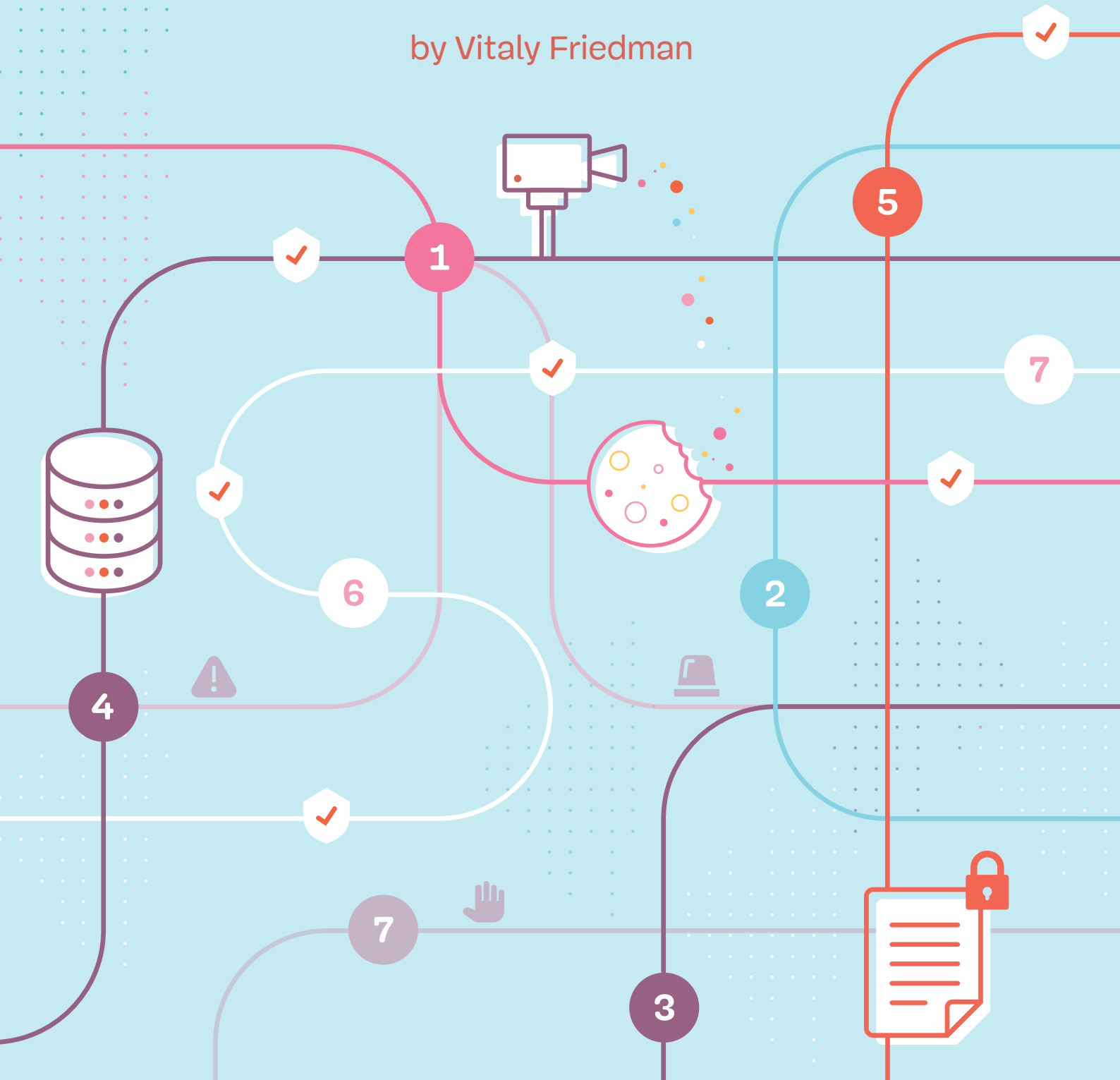
My personal thanks must go to everyone who has been involved in making this issue what it is. The design of the magazine is by Veerle Pieters, with additional illustration provided by Ricardo Gimenes and copy-editing by Owen Gregory.

—Rachel Andrew, editor-in-chief

THE PILOT

Towards Ethics By Default, One Step At A Time

by Vitaly Friedman



MANY CONVERSATIONS IN OUR INDUSTRY TEND TO CIRCLE around strong opinions and universal answers. Choosing a shiny new technical stack or sticking to an old-school paradigm; betting on a trendy framework or building a custom light framework of your own; using an attention-grabbing pop-up or sticking to calmer, less annoying solutions.

We tend to have strong opinions about design and development, and so we agree and disagree, and argue endlessly, trying to protect and explain our views. Sometimes (and maybe a bit too often) to the point that conversations escalate and result in annoyingly disgruntled camps not agreeing on *anything*.

1

It's not the stubbornness that brings us there though. It's the simple fact that we all have different backgrounds, expectations, and experiences when dealing with a problem. But sometimes we end up debating answers that are all acceptable and seeking the ultimate truth in a place where it really can't exist.

This pattern shows up for the usual suspects: accessibility, performance, tooling, workflows, and naming conventions. It also repeats itself with topics that are often considered to be ephemeral: ethics and privacy.

In the past, these areas could be spotted sporadically on the remote fringes of Twitter threads and blog posts; these days we've become very aware of the frightening dimensions that collection and use of personal data have silently gained. So we've started fighting back. Fighting back by publicly complaining about privacy-related dark patterns, unsolicited emails, shady practices, strict legal regulations, and ad-blocker wars against disruptive ads from hell.

Don't get me wrong: these are all important conversations to have and raising awareness matters. But perhaps we are missing an applicable, pragmatic approach for designing and building ethical and respectful interfaces within our existing, well-established processes.

If we ask ourselves why "honest" interfaces haven't made a breakthrough yet, bypassing and pushing away all the culprits out there, it might not be easy to find an answer at first. It's not that designers want to manipulate customers, or that developers want to make experiences slower, or that marketing people want to achieve quick wins at the costs of disrupting and annoying users' experience. It's that we know too well what solutions used to work in the past, yet we have no idea what might work even better.

What we are missing is a clear, affordable strategy for meeting business requirements without resorting to questionable practices that proved to be effective in the past.

In fact, we tend to rely on predictable A/B tests that give us clear answers for measurable, quantifiable insights. But when it comes to ethics and the long-term impact of an interface on loyalty, we are out there in the blue.

What we are missing is a clear, affordable strategy for meeting business requirements without resorting to questionable practices that proved to be effective in the past.

In most conversations I've had with marketing teams over the years, the main backlash against all the UX-focused, customer-protective changes in marketing was the simple fact that marketing teams didn't believe for a second that they could be as competitive as good ol' workhorse techniques.

So while, of course, calm, ethical and privacy-aware interfaces would benefit the user, moving away from the status quo would massively hurt business and make companies less competitive. Sadly enough, they might be right. Most of us use well-known services and websites that have all the despicable practices we so love to hate.

Tracking, collection and manipulation of data are at the very core of their business models, which allow them to capitalize on it for advertising and selling purposes. In fact, they succeed, and for many users, trading privacy is an acceptable cost for all the benefits that all those giants provide for nothing.

Beyond that, moving away from these benefits is remarkably hard, time-consuming, and just plain painful, so unless a company hurts its users on a level that goes way beyond gathering and selling data, they are unlikely to leave.

Many of you might remember the golden days when the first mobile interfaces were clunky and weird and slow, and when everything seemed to be out of place, and we were desperately trying to fill all those magical rectangles on shiny new mobile phones with adaptive and pixel-perfect layouts.

Despite good intentions and wondrous ideas, many of our first interfaces weren't great; they just weren't good executions of potentially great ideas.

> **I strongly believe that taking good care of users' data might be a competitive advantage and a unique selling proposition that no other company in your niche has.**

As time passed, these interfaces slowly disappeared, replaced by solutions that were designed better — slowly carved out of thorough efforts in research, testing, and gradual, ongoing refinements. It's rare that we see and regularly use some of those old interfaces today. Sometimes they remained locked up in app ecosystems, never updated or redesigned, but the competition pushed them away hastily. They just aren't competitive enough. Just because they weren't comfortable enough to enable users to reach their goals.

I wonder if the same will happen with the new wave of privacy- and ethics-aware applications that we see appearing today. Well-designed, small applications that do small tasks very well, with a strong focus on ethical, respectful, and honest pixels, without shady backdoors and psychological tricks. We can't expect giants to change overnight, but once these alternative solutions start succeeding, they might be forced to refine their models in response. I strongly believe that taking good care of users' data might be a competitive advantage and a unique selling proposition that no other company in your niche has.

For that to happen, though, we need to understand common pain points that users might have, and establish interface patterns that designers and developers could easily use. It could be a growing repository of inclusive, ethical patterns and components for various frameworks, with solutions and checklists to use on a daily basis. Privacy By Design[1] is one of the frameworks that goes in the right direction.

We might not agree on many things in the industry, but when it comes to ethics and privacy, we all have the same goals: produce respectful, honest interfaces while solving business requirements well and efficiently. To get there, rather than complaining about poor examples of infected, ignorant, and disrespectful interfaces, we need to explore all the little touchpoints that make up a wonderful, honest experience:

- Inclusivity and accessibility baked in by default, with components not getting broken by heavy inaccessible frameworks.
- Best practices for designing notifications UX, permissions UX, location tracking UX and not-so-notorious pop-ups.
- Best practices for designing interactions for GDPR/cookie-consent pop-ups as well as appropriate off-the-shelf tooling.
- Techniques for providing and adjusting privacy settings, with smart defaults, presets, labels and iconography.

1. *http://smashi.ng/privacybydesign*

> **We just need to start shifting the conversations from universal, all-or-nothing approaches towards practical strategies for making interfaces more honest and ethical, one step at a time.**

- Practices for designing offboarding experience: that is, experiences customers have when leaving a site or a service. It would involve dealing with users' data, exporting data, and deleting data.
- Strategies for dealing with sensitive private information such as gender, age, birthday, and phone number, and how to request even more sensitive data, such as passport number or social security number (if needed for verification purposes).
- Best practices to design interfaces that require access to geolocation and camera, and how to enable users to revoke and adjust the settings later on.
- Guidelines for designing integration with third-party services and how to explain to customers what will happen to their data.
- Design patterns to create better UIs for children, older people, and disadvantaged users while respecting and protecting them and their data. That alone isn't enough, though.

We also need to explore how we can make honest interfaces the default in most projects, legacy and brand-new alike, and that means figuring out how to integrate ethical considerations into existing processes and frameworks. As the industry, at this point, we have to consider:

- How ethical approaches can meet and drive business requirements, while keeping the product competitive on the market.
- How we can integrate ethical design patterns into widely spread content management systems and frameworks.
- How browsers could adapt their behavior to protect users' privacy.
- How to measure the long-term impact of ethical and privacy-aware practices, and what metrics to use to quantify them.
- How to transition legacy projects and business logic from gray practices to a new ethical framework while not ruining the business along the way.
- Successful case studies that highlight the financial and engagement-related long-term benefits of ethical designs.

Big changes usually happen from small, continuous refinements. Of course, our goal is to create interfaces that hit all the right marks in terms of ethics and privacy, but the way there is a long one, and it's not just a switch you can flick easily. It's a process that would require years to complete.

We've done it before. We've done it with the rise of remarkably smart and beautiful interfaces in the last decade. We've learned how to design breathtaking buttons and gorgeous tables and glorious animations, and we've learned how to build accessible, performant, and reliable applications. So we can do it again. We just need to start shifting the conversations from universal, all-or-nothing approaches towards practical strategies for making interfaces more honest and ethical, one step at a time.

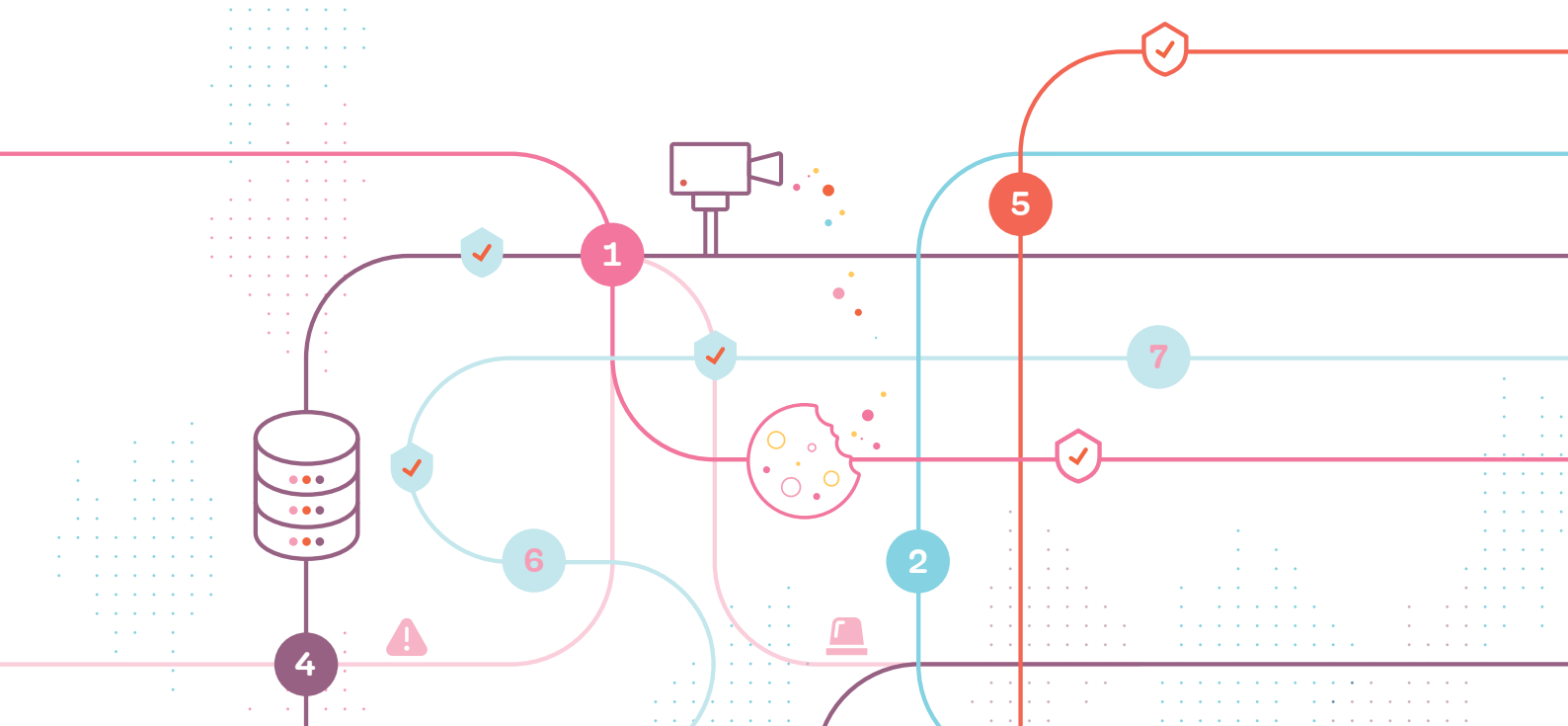
On the following pages, we'll try to pave the path for a more considerate and respectful landscape on the web; we'll try to find answers to at least some of the questions raised above.

We will need your help to turn it into something much bigger, though — something that would shape how the web will evolve over the years to come.

It's an exciting time to figure out a solution to a problem that is ubiquitous and desperately needs solving. Personally, I can't wait to contribute and be involved in these conversations.

ABOUT THE AUTHOR
Vitaly Friedman

Vitaly Friedman loves beautiful content and doesn't like to give in easily. When he is not writing or speaking at a conference, he's most probably running front-end/UX workshops and webinars. He loves solving complex UX, front-end and performance problems.



A Look Back At 2018

2018 WAS A GOOD YEAR FOR SMASHINGCONF, where we organized five great events. These conferences took place in London, San Francisco, Toronto, Freiburg and New York. It was also very much a year where we thought about what we were doing and how we were doing it. And we're trying to make it even better in 2019. Toronto was a special one last year. It was the first time in this new city, which is always exciting and scary at the same time. To make matters even more interesting it was also the first time we used the *no-slides* format. *No-slides* means a lot of live designing and coding sessions on stage, so all sessions are live and interactive. This turned out to be a huge success, both attendees and speakers really loved it, so we decided to keep on using the format.

> **I'm now seriously considering this format as a way I do talks at other conferences.**[2]
>
> — Dan Mall

2. *http://smashi.ng/smashingconfdan*

We organized SmashingConf Toronto in the movie theatre TIFF Bell Lightbox, which is a lovely theatre that could hold 400 people yet still felt cosy. When we look for SmashingConf venues, we want them to have character and be interesting.

At the same time they must check a number of boxes such as the number of seats, the right location with great lunch options nearby, all the right audio-visual equipment, and so on.

> **From an attendance point of view: I think this was the best conference learning experience.**[3]
>
> — Sara Soueidan

Team

Every conference is led by one person who takes care of the big things such as locations and catering. That also means the person who leads the conference is doing field research. During the year, quite often the team covers all time zones, which is inconvenient and useful at the same time. A good conference organization relies heavily on coffee and spreadsheets, supported by communication tools such as Slack and Skype. Good preparation in the months before the conference is absolutely vital, combined with proper teamwork just before and during the conference itself.

Most of the team members fly in a few days before the conference. We have breakfast together when we discuss last minute details, and even brainstorm for the next conference. These meetings tend to happen at a nice coffee place, because Vitaly likes fancy coffee places and the rest of the team don't mind at all. And then we go and do our duties: checking the venue, meeting with volunteers, and sending a lot of last-minute emails. The days before the conference are quite hectic, when we get everything ready for the workshops, our speakers arrive and we do final checks on a lot of details. The evening before the conference we run the preconference warmup, and just a little later the speakers' dinner starts.

On the day itself, everybody has their own role: You will find Vitaly standing on stage, or just right next it. He has an overview of the whole operations and stage management. Besides that, he generally comes up with new ideas all of the time.

Amanda is our AV resident, sitting in the back behind a laptop, making sure everything displayed on the screen looks perfect. She also produces our Toronto and New York events.

3. *http://smashi.ng/smashingconfsara*

If you see a woman running around with a smile on her face, it's likely to be Mariona. Probably that's because she is having fun, but possibly also because she just drank too much matcha tea. She takes good care of the sponsors and knows her way around in San Francisco, too!

It's quite likely you'll find Jan behind badges. He is a Freiburg resident and has been with SmashingConf for a long time.

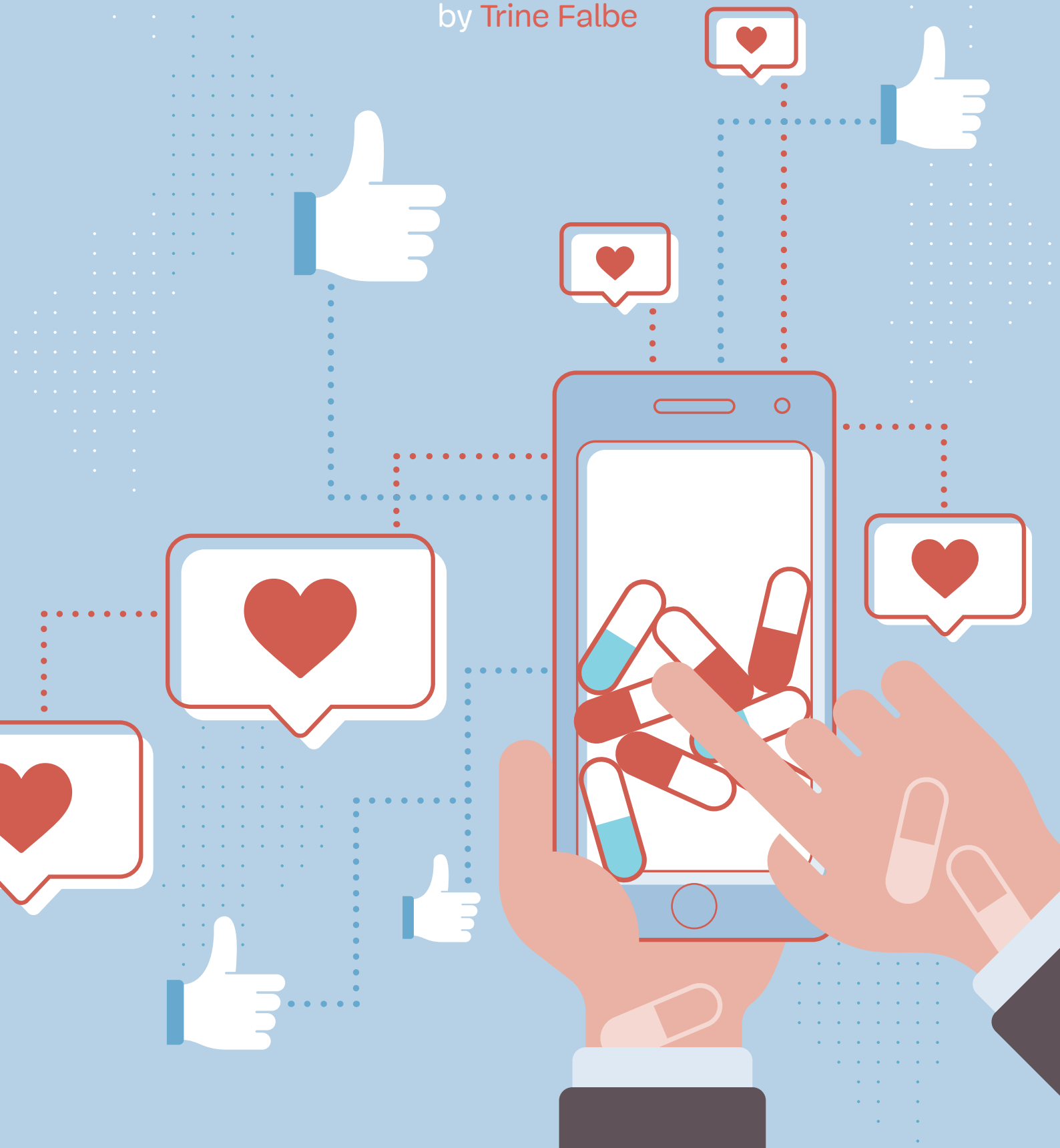
Charis is the newest kid on the block. You'll find her taking care of the social media and website. But she is also quite likely the last woman standing at the after party, as someone has to make sure we all leave, right? And if you see somebody running around and taking photos, that's Marc, who is our house photographer. Don't forget to smile.

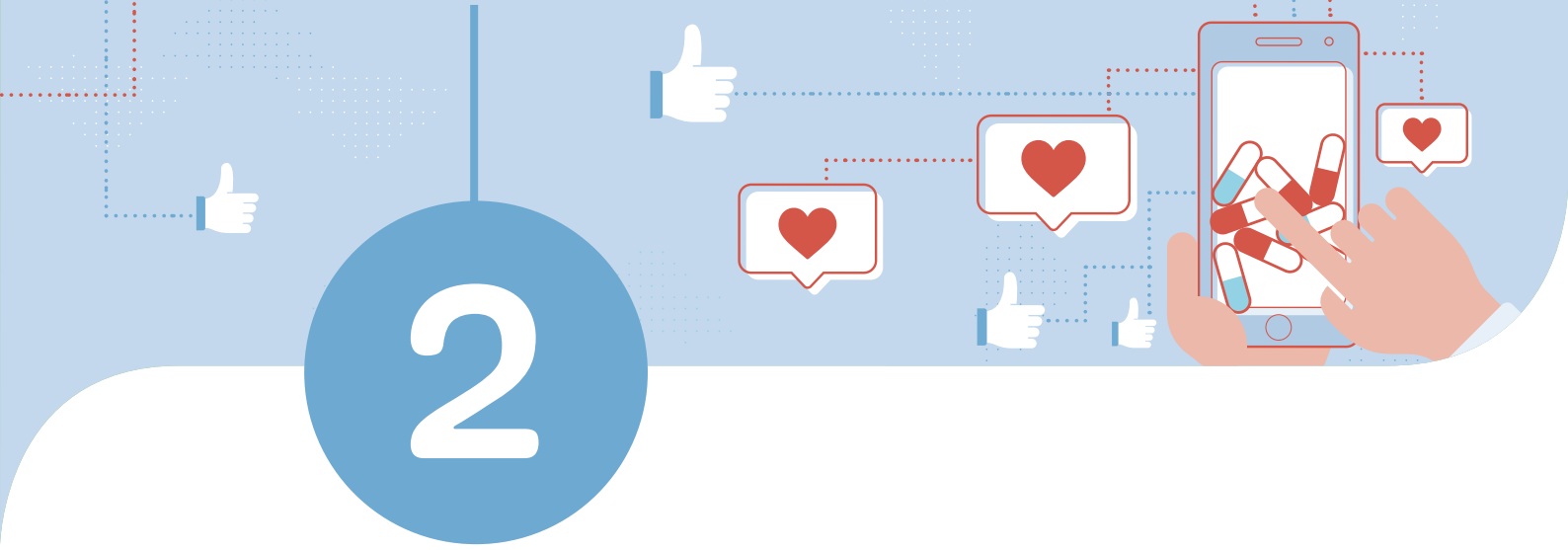
Once the conference is properly running and everybody is in, AV and Wi-Fi works, sponsors are properly set up and the catering has prepared us with coffee, tea and snacks, we all get a bit more relaxed. We still don't sleep very much during those days, but at least we can usually enjoy the atmosphere, interacting with the speakers and attendees.

Once the conference is over, and we have a little bit of time left, we try to squeeze in a touristy trip, such as visiting the Niagara Falls, museums or go to a concert. Once we get home, we sleep a lot! And then we move on to the next one.

Designing For Addiction

by Trine Falbe





2

I NOTICE HIM AS I WALK DOWN THE street towards the city square. He sits on the ground on a blanket with a beautiful, caramel-colored dog next to him. She looks like a Shar-Pei mix (the dog with all the wrinkles) and I resist the urge to pet her right away.

I walk up to them to buy a copy of Hus Forbi, a street newspaper sold by homeless and socially vulnerable people.

We chat for a bit. His name is Peter. He is homeless and a former drug addict. His dog is his everything, and she loves to cuddle.

Peter's story is not different from many other homeless people. He grew up in an abusive household and turned to drugs at a young age to cope with life. This eventually led to him losing his home. After nearly dying from an overdose, he is now clean. Before getting clean, drugs were the first thing he thought about when he opened his eyes in the morning, and the last thing on his mind at night.

I stand up after having cuddled Peter's dog for a while. It's dinner time, and she turns her attention to the dog food lovingly served by her owner.

Device addiction is noticeable everywhere, in the private and public space alike.

Looking up to the busy street around me, I notice the other addicts. Staring at their shiny screens, oblivious to the people they pass, and even to their children in the strollers in front of them. Check, reply, like, repeat.

The fix these people seek is of a different nature to the one Peter used to chase. Nevertheless, their brains are addicted. The urge for the dopamine that infuses the brain with every social validation, and submission to the fear of missing out, is strong. And while Peter's drugs are illegal, the drug these people use is not. Often, it even comes for free, if they give up their lives in the name of big data.

We who work in the digital industry might not be in daily contact with people like Peter. The addiction we create, nurture, and are often victims of ourselves, is of a different kind than the addiction Peter used to have. However, we are the pushers of drugs to the increasing number of device addicts in the world through the products we make.

The consequences of device addiction

Research is not conclusive on how many times per day people check their phones, but numbers range from 75 to 150 times per day. That is roughly anywhere between five and ten times an hour, if we assume that the average person is awake for 16 hours each day. And while the many positive changes that smartphones have brought to our lives should not be diminished, there is a flip side.

Digital products feed addiction

According to research that came out of the University of Texas in June 2017, the mere presence of a smartphone significantly reduces our cognitive capacity. Using a smartphone or tablet just before bedtime can make falling asleep more difficult because of the blue light from the screen. And the omnipresent access to a Google search is said to make us lazy thinkers, less capable of analysis and reflection.

People who get addicted to their devices are essentially enslaved by the mechanics of the engagement features. Social media platforms like Facebook and Snapchat exploit our fear of missing out (FOMO). They also take advantage of our urge for social validation. We like to feel loved, acknowledged and respected. We also like to feel happy, because that too releases dopamine in our brains.

The success of social media platforms and their engagement mechanics has been widely accepted and picked up by other digital products. Unless we specifically turn them off, we are notified by the majority of the apps installed on our devices. And this adds to the many problems related to device addiction.

> **People who get addicted to their devices are essentially enslaved by the mechanics in the engagement features.**

Devices don't kill people; people kill people

A quarter of all traffic accidents in the US are caused by drivers distracted by their mobile devices. A member of the National Rifle Association (NRA) might claim with a straight face that an accident isn't the fault of the mobile device — rather, it is the fault of the person driving the car.

Of course, a gun's purpose is to wound and kill; a smartphone isn't manufactured to distract drivers and cause injury. But we have to acknowledge the risk we impose on the people who use the products we make. We cannot separate the digital products we create from the devices they are used on. When we make an app, we make part of a device.

Parents' use of devices affects child development

According to a 2018 study[4] published by the international journal of science Nature Research, parents' excessive use of digital devices affects a wide range of components in their children's development. Parents' use of devices was proven to cause more extreme behavior in children, such as acting out to get attention or turning inward to find what they could not get from their parents. Language acquisition was also proved to be affected, as device-addicted parents tended not to respond verbally to the children to the same extent as parents who were not constantly occupied by a device.

Learning and staying focused is hard in the digital age.

There are a lot of examples of universities and higher education institutions around the world that have chosen to ban mobile devices and social media in the classrooms because they found students to be so distracted by them that it affected their learning negatively.

At Business Academy Aarhus in Denmark, a two-year experiment was carried out in 2015–2017 with two groups of students on the marketing and economics program. 300 students were enrolled, and of those, 60 students were told not to use any devices during the school day. Devices were only allowed when they had a direct purpose, such as using a computer to write a document or researching online. Phones were to be put away at all times.

The 60 students had the lowest grade level on entry into the program. After two years, they graduated top of the class of 300.

When asked, more than 90% of the 60 students said that the experiment had had a positive effect on their motivation and engagement in the class.

The results are staggering, but not surprising. If we assume that the students in the experiment avoided checking their phones five to ten times per hour while at school, they are bound to have had much more mental space for focusing on the subjects and collaboration with their peers.

4. *http://smashi.ng/technoference*

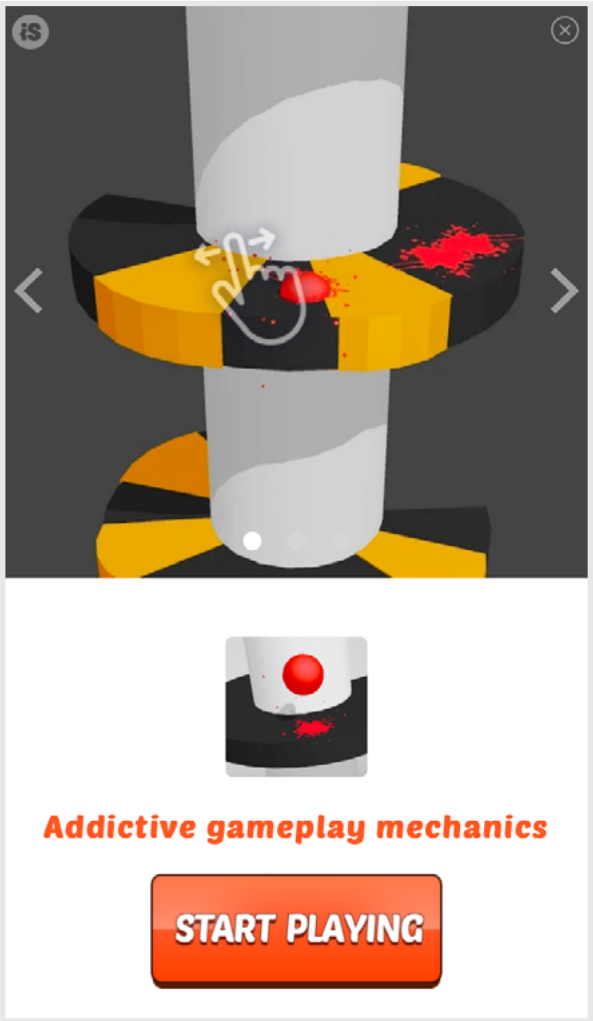
Behavior change for better or worse

BJ Fogg,[5] an expert in behavior change based at Stanford University, talks about three factors that must be present for a behavior to occur: motivation, ability, and trigger. For someone to do something, they must be motivated to do so, for instance by the promise of pleasure, social acceptance, or the hope that something good will happen. They must also be able to perform the behavior, which means it must be simple enough for them to do, either from a financial, time or physical perspective. Finally, there must be a trigger which prompts the behavior. In the digital space, a trigger is often a call to action, or a notification.

To illustrate how behavior works according to Fogg, let's take a product example. MobilePay[6] is an app developed by Danske Bank, the largest bank in Denmark. It allows people to easily wire money to others just by knowing their mobile phone number.

Over 90% of all smartphone owners in Denmark have MobilePay on their phones. Why?

- **Motivation**: the overarching problems of small transactions between friends for coffee, when buying things on secondhand markets, and for small businesses to offer digital payments without having to invest in expensive systems.
- **Ability**: the app is free (without ads!), and all you need is a credit card and a phone number to use it.



Close buttons in mobile ads are often purposefully designed too small to tap.

- **Trigger**: "Do you have MobilePay?" is a very common question when someone pays for others; for instance, when buying a shared gift for a colleague. Signs at the cash register in shops and at flea markets are also triggers.

5. *http://smashi.ng/bjfogg*
6. *http://smashi.ng/mobilepay*

We can choose to use this knowledge of how behavior change works for either good or ill. Unfortunately, it is commonly used to increase engagement in digital products in ways that encourage device addiction.

Excessive notification frameworks seen in social apps are carefully designed to increase the amount of times people open and check or interact with the app. These notifications take advantage of all the mechanisms within our brains that get attracted and addicted to social validation and the fear of missing out on important things.

As is the case with the knowledge of behavior change mechanics, all design and interaction principles can be used for good or ill. To play with that thought for a moment, let's look at Fitts's law. Fitts's law predicts that the time it takes to move to a target is a function of the ratio between the distance to and the width of the target. In digital user interfaces, precision is also a success metric. The larger the touch target, the higher the success rate of hitting the touch target precisely.

An understanding of Fitts's law can be used for two things: it can help us design an interface with touch targets big enough for our users to succeed in clicking or tapping every time; or it can help us create a touch target so small that users are likely to miss it and instead click the area next to the target, like an ad. This is the case for many mobile ads.

Mindful products through less obstruction

It is common for people who work in product engagement to use terms like getting users "hooked" or "addicted." This in itself is a problem, as the rhetoric shapes our behavior and mindset.

What if we started considering users as people to "cater to," instead of seeing them as subjects whom we aim to hook and addict? People who choose to use our product, because it improves a tiny bit of their lives? That alone would be a good starting point, because it builds empathy. Empathy makes it much harder to close our eyes and pretend we don't see if the people we cater to are mistreated. It makes us capable of feeling their pain.

A starting point to creating more mindful products is to reduce the amount and rate of notifications. Apple's Human Interface Guidelines[7] suggest that notifications be kept useful and informative, and that notifications are not repeated for the same thing, even if the user hasn't responded.

> **Whenever you consider adding a notification to the framework, ask yourself if it is useful. If the answer is yes, but only to the business, then the real answer is no.**

7. *http://smashi.ng/humaninterfaceguidelines*

Focus on the true product value

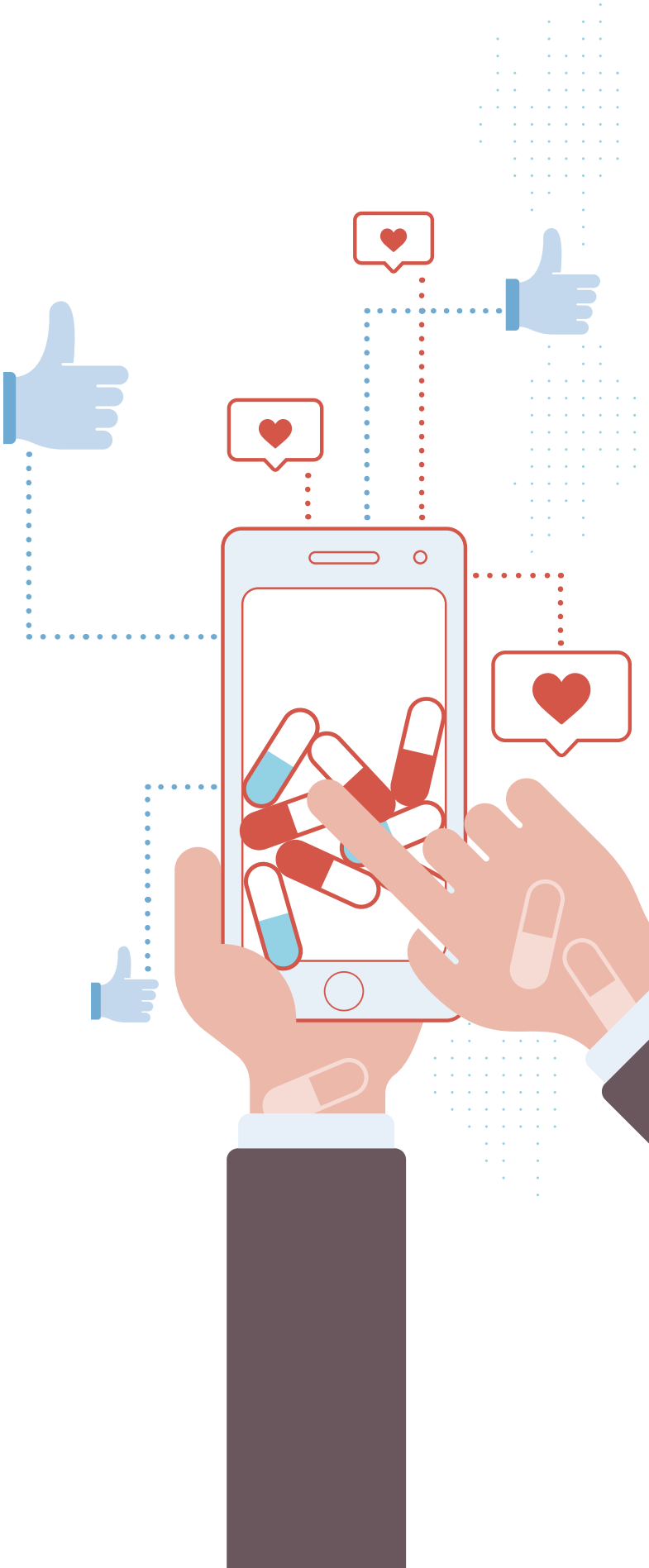
If a product can only increase engagement by adding addictive notifications, the product has a problem. It is not adding enough value to the people who use it. So maybe it's time to look at that instead of adding mindless notifications.

To create truly empowering products that people use willingly, it is worth looking at the value instead of the behavior triggers. This happens by asking the tough questions. What value does our product deliver? What problems are we solving? Why should people even bother using our product?

The true answers to these questions are found among the people you cater to. So go out there. Talk to them. Involve them. And most importantly, respect them. Only then will you be able to build products they will want to use — on their own terms.

ABOUT THE AUTHOR
Trine Falbe

Trine Falbe is a UX strategist, consultant, speaker and lecturer focused on empowering people through ethical design.
trinefalbe.com



Our Lovely Smashing Books

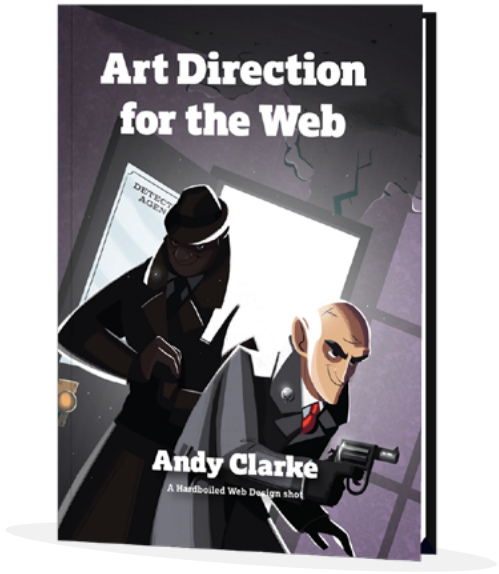
QUALITY MATTERS. OUR PRINTED BOOKS ARE crafted to deliver in-depth knowledge and expertise shared by experts and practitioners from the industry. If you prefer your reading in digital form, our printed books are all available as eBooks, plus we have a number of ebook-only editions, often covering key industry information, and written by leading experts. Smashing members can access the whole Smashing eBook Library as part of their subscription.

Art Direction for the Web

by Andy Clarke. Published in April 2019.

In this book, you'll learn about art direction; what it means, why it matters, who can do it, and — most importantly — how it applies to the web. It's for web designers and developers who want to understand art direction and how to make it work for digital products and websites.

Keywords: CSS Grid, Flexbox, art direction



> *On the web, art direction has been a dream deferred. "The medium wasn't meant for that,' we said. We told ourselves screens and browsers are too unreliable, pages too shape-shifty, production schedules too merciless to let us give our readers and users the kind of thoughtful art directional experiences they crave. But no longer. Andy Clarke's Art Direction for the Web should usher in a new age of creative web design.*
>
> *— Jeffrey Zeldman, creative director at Automattic*

> *Andy shows how art direction can elevate your website to a new level through a positive experience, and how to execute these design principles and techniques into your designs. This book is filled with tons of well-explained practical examples using the most up-to-date CSS technologies. It'll spin your brain towards more creative thinking and give your pages a soul.*
>
> *— Veerle Pieters, Belgian graphic/web designer*

Recent Additions To The Smashing Library

Form Design Patterns

by Adam Silver. Published in October 2018.

At first glance, forms are simple to learn. Made up of just a handful of inputs, you can create a form in little time. But when we consider the journeys we need to design; the users we need to design for; the browsers and devices of varying sizes, capabilities and bugs; and ensuring that the result is simple and inclusive — then form design becomes a bigger and far more interesting challenge. *Form Design Patterns* helps you get a firm handle on them.

Keywords: web forms, design patterns, HTML

> *I have been writing forms in HTML for over 20 years. This book captures the essence of what it is to embrace standards, progressively enhance and deliver simple, accessible forms. By formalizing design patterns we can all use and implement, developers and designers can focus on their website and product. I wish this had been available 20 years ago!*
>
> *— Paul Duncan, design technologies and accessibility teacher*

> *In a world of horribly marked-up forms, this book is a beacon of light illuminating the way to more accessible user experiences. I highly recommend it to anyone designing or developing user interfaces to avoid the common form accessibility pitfalls we see all too often.*
>
> *— Marcy Sutton, accessibility advocate*

Smashing Book 6: New Frontiers In Web Design

by the Web Community. Published in September 2018.

Smashing Book 6 explores how to build accessible single-page apps with React or Angular, how to use CSS Grid Layout, CSS Custom Properties and service workers, as well as how to load assets on the web in times of HTTP/2 and bloated third-party scripts.

Keywords: front-end, UX, usability, VR/AR, design

1. Making Design Systems Work In Real-Life
By Laura Elizabeth

2. Accessibility In Times Of Single-Page Applications
By Marcy Sutton

3. Production-Ready CSS Grid Layouts
By Rachel Andrew

4. Strategic Guide To CSS Custom Properties
By Mike Riethmueller

5. Building An Advanced Service Worker
By Lyza Gardner

6. Loading Assets On The Web
By Yoav Weiss

7. Conversation Interface Design Patterns
By Adrian Zumbrunnen

8. Building Chatbots And Designing For Watches
By Greg Nudelman

9. Cross Reality And The Web (AR/VR)
By Ada Rose Cannon

10. Bringing Personality Back To The Web
By Vitaly Friedman

The books published by SmashingMag and team are getting better each time. I was thrilled to be able to preview it... every chapter is good! Having focused on a11y for much of my career, Marcy Sutton's chapter is a personal favorite.

— Stephen Hay, author of Responsive Design Workflow

Just got the new Smashing Book 6 by SmashingMag. What a blast! From CSS Grid Layout, CSS Custom Properties and service workers all the way to the HTTP/2 and conversational interfaces and many more. I recommend it to all the people who build interfaces.

— Mihael Tomić, design lead at Mono

It's Not About You

by Heather Burns and
Morten Rand-Hendriksen

IF YOU'RE HOLDING THIS MAGAZINE IN YOUR HANDS, YOU KNOW that ethics is the tech trend for 2019. That's a good thing – or is it? A cautious reader might stop to ponder why ethics is seen as a trend at all. After all, trends – like fashion – go in and out, and last year's trend is this year's laughing stock. As we spend 2019 shifting our gazes from gadgets to governance, we need to make sure we are not appropriating the ethics trend as the latest fashion, as if it's something to make us look good now but foolish later. We also need to make sure we are not using the ethics trend to cover for our shortcomings elsewhere, particularly where privacy is concerned. After all, who would look cynically at a project making a big noise about privacy ethics?

Well, we all should.

3

It's time to talk about "ethics washing." It is an academically recognized phenomenon largely focusing on, but not limited to, privacy law and regulation. Loosely put, ethics washing[8] is what happens when ethics projects are devised and adopted in lieu of a healthy approach to legal compliance. These codes are rarely deployed to complement privacy laws and the rights they grant users; instead, they are often used to circumvent them.

It's no surprise that privacy ethics washing has hit the mainstream. Ethics, after all, are often misunderstood as soft and fuzzy, and talking about them makes you look good. Laws, on the other hand, are often misunderstood as hard and scary, and talking about them makes you look rather dull. But when it comes to online privacy and user protection, using ethics washing to dodge rights and regulation is a trend which will ultimately backfire on us all.

8. *http://smashi.ng/ethicswashing*

What's the problem with ethics washing?

Ethics washing is based on a fundamental misunderstanding of the meaning and purpose of ethics as a craft and science. According to the Markkula Center for Applied Ethics, whose work on ethics in technology practice[9] is industry-leading, "Ethics is based on well-founded standards of right and wrong that prescribe what humans ought to do, usually in terms of rights, obligations, benefits to society, fairness, or specific virtues."[10]

For this reason, discussions on ethics and privacy regulation tend to focus on the moral causes for why they are important (for example, "Privacy is essential to protect the individual's right to freedom"), deferring to the law to define what that means. In this view, ethics inform legislation. But ethics washing uses poorly defined (and often misunderstood) ethics as a tool to supplant legislation, effectively putting the cart before the horse while denying that the horse exists in the first place.

The fact that ethics washing in privacy exists at all is a testament to how poorly online privacy legislation is understood and respected, even by those who make the web itself. Contrary to the tired trope which depicts the internet as an unregulated wild west, a rainbow of privacy and data protection laws have existed in most countries since the 1990s. 2019 will see a federal privacy law devised, in some shape or form, in the United States, the last major holdout against comprehensive privacy legislation. Put simply, if your work has not been constrained by privacy law before, it will be soon.

Ahead of its implementation deadline in May 2018, our work in educating digital professionals about GDPR — the European Union's privacy law overhaul — taught us that the companies which had the most work to do were the ones who had not been in healthy compliance with existing privacy regulations in the first place. It also taught us that the digital professionals who scream the loudest about the impossibility of compliance with privacy laws are the ones who have — to put it politely — stretched those laws past their limits, and do not like being told the party's over.

In cases like these, where digital companies have been caught short of their existing obligations under privacy laws and regulations, starting inclusive discussions about ethics can be a

9. *http://smashi.ng/ethicspractice*
10. *http://smashi.ng/whatisethics*

> **Thanks to ethics washing, what we see are public pledges of ethics being used as a cover for broken laws and regulations. That does not seem very ethical at all.**

great way to catch up in plain sight. After all, that's what ethics are for: taking a step back and looking at how our decisions impact the world and whether they lead us toward a world where human flourishing is possible. But used as a tool for risk mitigation, a cursory wash of ethics can, in a manner which would make the slickest politician proud, lead to the "discovery" of privacy obligations written in law,[11] and the rewording of them into ethical standards which are loudly proclaimed as their own inheritance.

This color of privacy washing blurs the lines between what is explicitly constrained by law, which has externally accountable definitions, and what is adopted within projects as internally policed codes of conduct. This is also known as "marking your own homework," and at its worst, it allows projects to use what they call ethics to violate legal obligations. The most striking example of this was Google's DeepMind project, which collected and shared the health data of 1.6 million patients of the UK's National Health Service without either patient consent or a legal basis to share that data.[12] Despite being caught, project representatives still claimed with a straight face that working to support the NHS made it an ethical project using ethical data for ethical purposes.

The race to the bottom

The wonderful thing about privacy law is that it has your back. Codes of ethics do not. Ethics do not provide a guarantee of action, nor are they tied to external enforcement on their own. They play a subtly different role: codes of ethics can be used as part of a design and development process, and can be used to help form and validate internal guidelines which individuals, teams, and organizations make a choice to follow. We see this in academic research and in organized industries like engineering and medicine. But without an agreed set of ethical standards for an accountable industry body to use to adjudicate potential violations, codes of ethics remain an internal tool whose value stands and falls on each worker's willingness to follow them.

In that regard, using codes of ethics as a substitute for accountability to public and private governance is an abuse of ethics. This color of ethics washing actually increases governance risks. It creates a dangerous race to the bottom where projects compete to adopt the vaguest, weakest, and most privacy-hostile practices possible, while framing their charitable gestures as a laudable achievement.

11. *http://smashi.ng/datalaw*
12. *http://smashi.ng/deepmind*

Yet privacy and governance, at all times, must be a race to the top. We are not above the law.

For those in the digital sector whose politics hold that there should be no politics, and who believe their projects are living in another world not quite part of our own, ethics washing allows the adoption of codes of practice which skim the surface of privacy law without ever touching it. There are two problems with this approach.

First, it signals a belief in self-regulation, using arbitrary ethics as the constraint, rather than an adherence to actual regulation using the rule of law as the constraint. Put another way, it is a declaration that a project, and the people who make it, are above the law.

Yet at a time when data protection and privacy scandals have governments around the world looking to regulate the web and privatize law enforcement onto those who make it — particularly where the policing of content is concerned — refusing to work within existing privacy regulations all but guarantees that new privacy laws will be more restrictive, more difficult, and more of a barrier to innovation than the relatively easy ones we have now.

Second, this color of ethics washing shifts the moral responsibility for protecting privacy from the project to the user — or rather, from the perpetrator to the victim — leaving the people who use our creations with all of the burdens and none of the recourse. Privacy law is about safeguarding and empowering users through fundamental human, citizen, and consumer rights. Washing privacy law into voluntary principles leaves users vulnerable to the personal ideologies of occasionally volatile project leaders who view the law, and the rights it grants users, as a threat to their power.

To put it bluntly, the only thing that will result from project leaders using ethics washing to hold themselves above privacy law is that we will all get dragged down with them. That does not seem very ethical either.

How can projects make sure that their privacy ethics are more than this year's fashion? Ben Wagner, a professor at Vienna University of Economics and Business who has written extensively on ethics washing in tech, suggests six tests[13] which should be applied to ethical initiatives and codes to ensure that they are not engaging in ethics washing:

1. There must be early and regular engagement with external stakeholders.
2. There must be a means of external, but not necessarily public, independent oversight.
3. There must be transparent procedures on why choices were made.
4. There must be a stable framework of non-arbitrary standards which can be used to reference the selection of certain values, ethics, and rights over other ones.
5. There must be a clear indication that the selected ethics do not substitute for fundamental human or citizen rights.
6. There must be a clear statement on the relationship between the principles declared and any existing legal or regulatory frameworks, including an explanation of what will happen if the principles and the law are in conflict.

A rising tide lifts all boats

Used correctly, ethics give us the tools to take a critical look at how we make decisions, and to determine whether our decisions grant users agency, rights, protections, and the opportunity to flourish. They can remind us that every decision we make is one made on behalf of other people, one that carves a path they follow into our shared future. They are so much more than a passing trend, and they are the key to making the web a better place for all.

Yet ethics do not stand alone. They merely lay the foundation for larger frameworks of social contracts encompassing policy, governance, law, and human rights. Discussing, defining, clarifying, and evolving those ethics, and the structures we build on them, is the job of everyone who makes the web. But it must be done in the right way.

Suggested Resources

Morten Rand-Hendriksen, *"Using Ethics in Web Design"*[14]

Ben Wagner, *"Ethics as an Escape from Regulation: From ethics-washing to ethics-shopping?"*[15]

Cenydd Bowles, *Future Ethics*, NowNext Press

Lucie Greene, *Silicon States: The Power and Politics of Big Tech and What It Means For Our Future*, Counterpoint

13. *http://smashi.ng/ethicsescape*
14. *http://smashi.ng/designethics*
15. *http://smashi.ng/privacylab*

The challenge facing us today, whether we are the largest social network or the loneliest digital worker, is how to align the values of our work more closely with the values of society as a whole. That cannot be achieved by misusing ethics to rationalize what we can get away with.

We owe it ourselves and our users to use ethics the right way to help shape the privacy rules and regulations which govern our craft, to differentiate between best practices and the rule of law, and to ensure the paths we carve for our users lead to human flourishing. And we owe it to ourselves to understand the important role ethics can play, and learn to use them to build better futures, rather than exploit the trend to use them as a loophole around the law and the rights it grants our users.

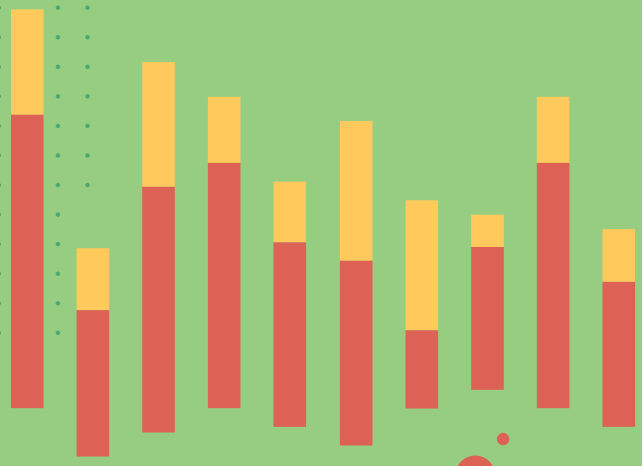
Tech ethics are the next stage of our industry's progression from adolescence to adulthood. To grow together, we must acknowledge that when ethics are washed into an alternative to privacy law or a substitute for fundamental rights, everyone — projects, users, and the industry itself — suffers in the end.

ABOUT THE AUTHOR
Heather Burns

We are people of enormous power and influence over the web. I empower digital professionals to use that power wisely. As a tech policy and regulation specialist, I educate the profession on the policy issues which impact our work, inspire professionals to participate constructively in the regulatory process, and facilitate cooperation between policymakers and project leaders.

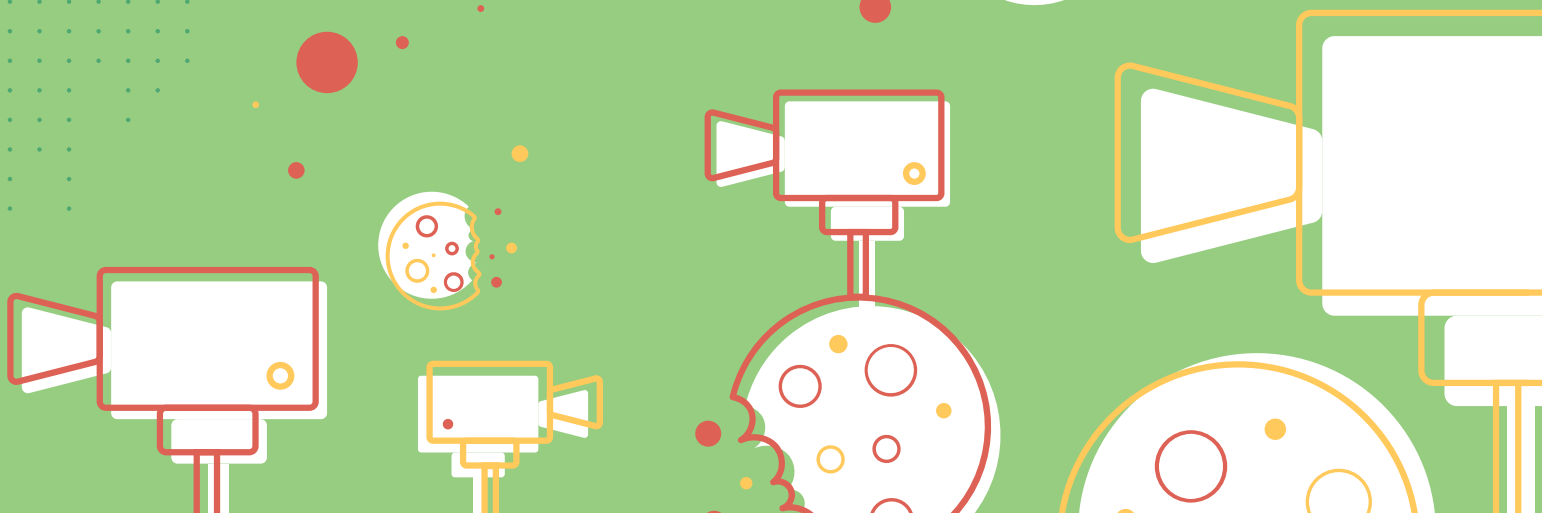
ABOUT THE AUTHOR
Morten Rand-Hendriksen

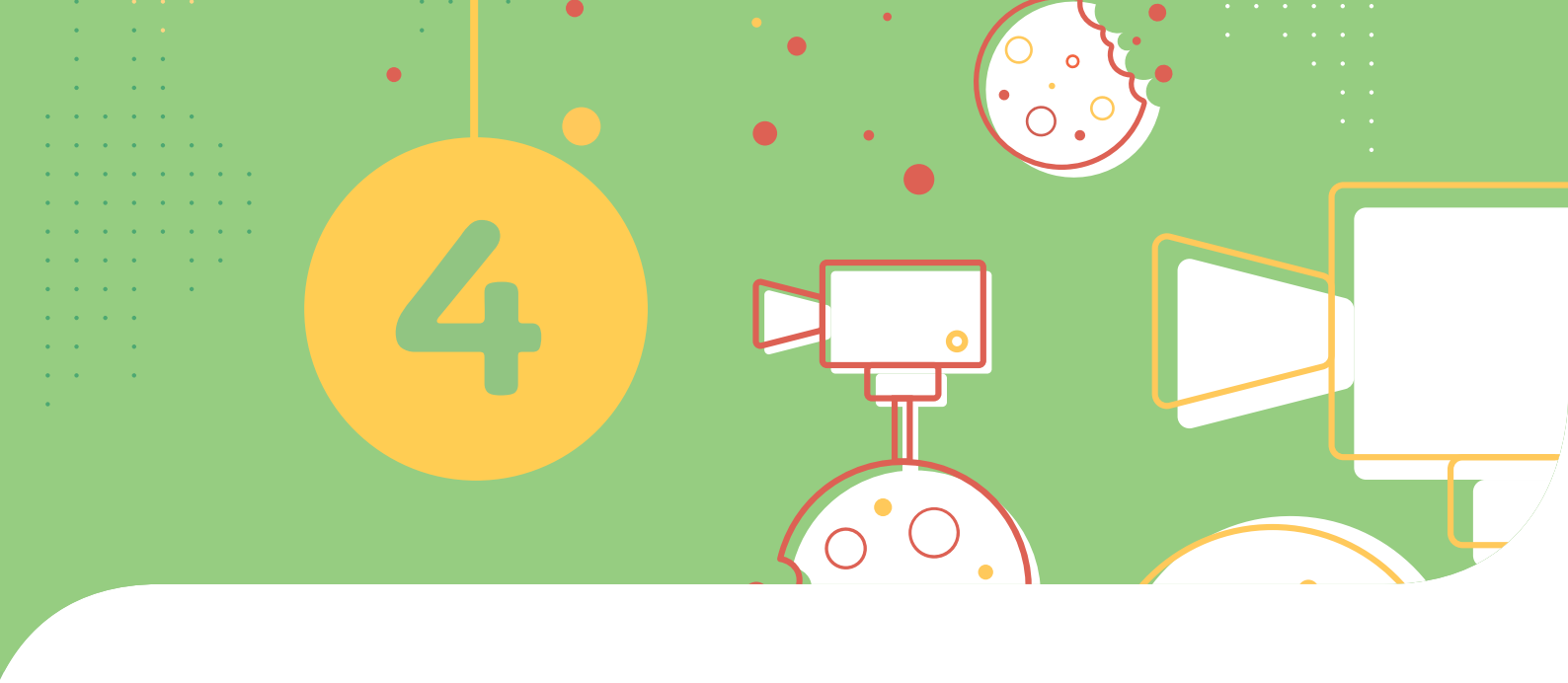
Morten is a senior staff instructor at LinkedIn Learning and Lynda.com with 60+ courses published on WordPress, web standards, design and UX, and future technologies. He also teaches interaction design at Emily Carr University of Art and Design, and contributes to WordPress core and community projects.



This One Weird Trick Tells Us Everything About You

by Laura Kalbag





PRETTY MUCH ANY RESOURCE ON THE web can track us. Every week I spend a couple of work days looking at trackers, trying to work out which of them are potentially harmful, and whether they should be blocked to protect people's privacy. It's a tricky task because nearly every tracker is potentially harmful.

We're mostly aware of how cookies and scripts can be used to track site visitors inside sites and across the web. Even without dedicated analytics, most server logs alone will record simple visitor information[16] (such as IP address and time of visit) by default. Folks working in marketing and social media may be aware of how images can be used as "pixel tags" or "web beacons" to collect information based on when the image is requested. Even the humble link becomes a tool for tracking when appended with an identifying query string.

It can be valuable to track visitors to provide functionality, such as keeping visitors logged in or remembering language preferences. But increasingly, tracking is used to collect data about us that is simply not necessary to the basic function of a website. The collection, sharing, and even selling of such data presents a serious threat to our privacy and other human rights.

It started with ads

Ads don't bother me much. It's the underlying tracking that's the problem. Ads in printed newspapers don't track their readers. The same is true for the web — an ad's image might be ugly or annoying, but it doesn't inherently compromise your privacy.

However, mainstream technology cannot sustain its business on the small returns from static ads. Venture capital is pumped into tech businesses with investors expecting huge returns on their investment. It's expensive to get a competitive product to market. On top of that, investors expect rapid growth to ensure a big pay day when the business gets its exit, goes public, or gets acquired

16. *http://smashi.ng/iplogging*

Advertisers in print media choose publications and pages based on audience demographics, not individuals.

by a larger corporation. The tiny number paid per click on static ads can't produce these levels of money or growth. In the early days of the web, ads evolved to use pop-overs, pop-unders and nauseating animation to attract your attention. When these strategies didn't result in more clicks and purchases, targeted advertising became the key to capture the user. Tracking individuals around the web helped advertisers build a sophisticated profile of a person's traits and behavior. Targeting enabled advertisers to create "relevant" ads — to entice particular traits, or based on previous purchases — making it more likely the ads would result in a sale.

When targeted ads became so effective for advertisers, it was inevitable other areas in tech would use targeting too. When the growth and success of a business thrive on data, you need to encourage more people to add more data. The best way to keep people hooked on your product is to deliver content you know will keep them connected. Showing posts your friends liked, popular posts, and geographically relevant posts all attempt to keep you checking your feed in case you're missing out. It feeds FOMO.[17] And it's why algorithmically generated social media feeds with infinite scroll are so successful (even though we say we hate them!). In the tech industry, we use the terms "capturing attention" and "increasing engagement" as euphemisms for addiction.

In the tech industry, we use the terms "capturing attention" and "increasing engagement" as euphemisms for addiction.

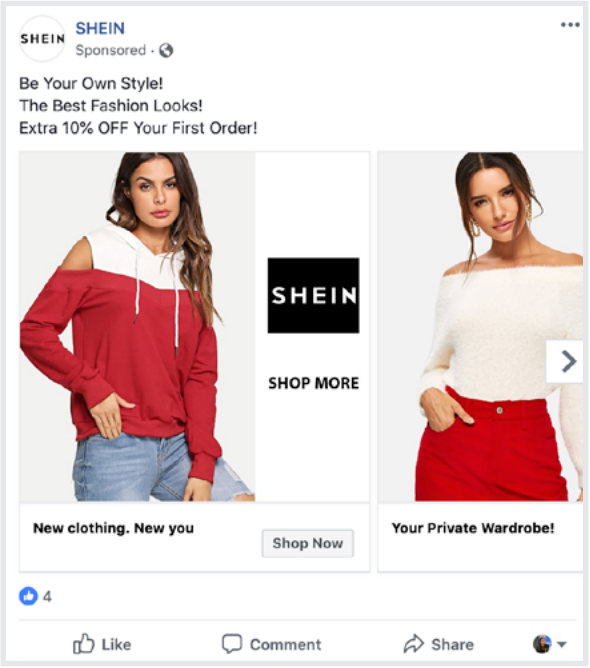
And now everything tracks us

Ultimately, tracking has shaped the business model for the majority of mainstream technology today. Shoshana Zuboff calls this model "surveillance capitalism."[18] Aral Balkan makes it clear who is being surveilled when he calls it "people farming."[19] Profiling individuals has proved so effective because trackers can easily obtain information about you from a wide selection of sources across the web.

17. *http://smashi.ng/definitionfomo*
18. *http://smashi.ng/survcapitalism*
19. *http://smashi.ng/sovereignty*

These profiles are accurate enough that the information is used to fuel all kinds of systems beyond e-commerce and social networks. Facebook got a patent for approving loans based on the credit ratings of your Facebook friends.[20] Health insurers use the data to decide premiums.[21] Data brokers sell the data to credit companies.[22] Governments can also get hold of the data for their own use.[23] And political parties can use the data to serve us personalized propaganda, affecting the outcomes of referendums and elections.[24] One charming man has made a service for men to deliver targeted ads to their partners to "convince them to initiate sex".[25] He said of his service:

> *It's unethical in many ways. But it's the business model of all media. If you're against it, you're against all media.*



I'm a woman in my thirties, so targeted ads show me clothes, hair styling accessories, and pregnancy tests.

The design decisions we make when we architect our sites have far-reaching implications. As Sara Wachter-Boettcher writes in *Technically Wrong*:

> *We hold technology in our pockets. We tell it our secrets. We rely on it to sustain relationships. It's the first thing many of us interact with in the morning, and the last thing we look at at night. Technology isn't just pervasive. It's personal.*

This pervasive and personal technology we build is used to manipulate people's behaviors and undermine democracy. This is why tracking is an issue of human rights. Even more so because the people who are most affected are those who are most vulnerable. *Queer Privacy* by Sarah Jamie Lewis is a book containing important examples:

> *The modern debate around privacy has been focused on its contention with security, and framed to be about terrorism and criminality. Lost in this debate are the very real day-to-day battles that we all face. Employees searching for new jobs without telling their boss, teenagers hiding partners from their parents, choosing what information to reveal on a dating profile; the list of times we actively choose what to reveal about ourselves is practically endless.*
>
> *Those scenarios take on more serious tones when we discuss marginalized populations: people of color, native indigenous peoples, queer communities, sufferers and survivors of domestic violence as well as disabled people, undocumented immigrants and others who dwell outside of the typical presented "norm."*

20. *http://smashi.ng/creditrating*
21. *http://smashi.ng/healthscore*
22. *http://smashi.ng/dataagainstpeople*
23. *http://smashi.ng/cisaact*
24. *http://smashi.ng/brexit*
25. *http://smashi.ng/inception*

What makes a tracker spy on you?

It's uncommon for a site to roll all its own custom functionality. It's easier to get a third party to provide a service where you just stick a chunk of code on your site. This means trackers are usually provided by a third party, and their ability to amass data is assisted by the diversity of sources. It also makes it easy to detect a tracker's presence on a site simply by looking at the third-party domains listed in the site's requests.

In November 2018, we[26] crawled 7,000 of the most popular sites on the web, and found the most prevalent trackers fall into the following categories.

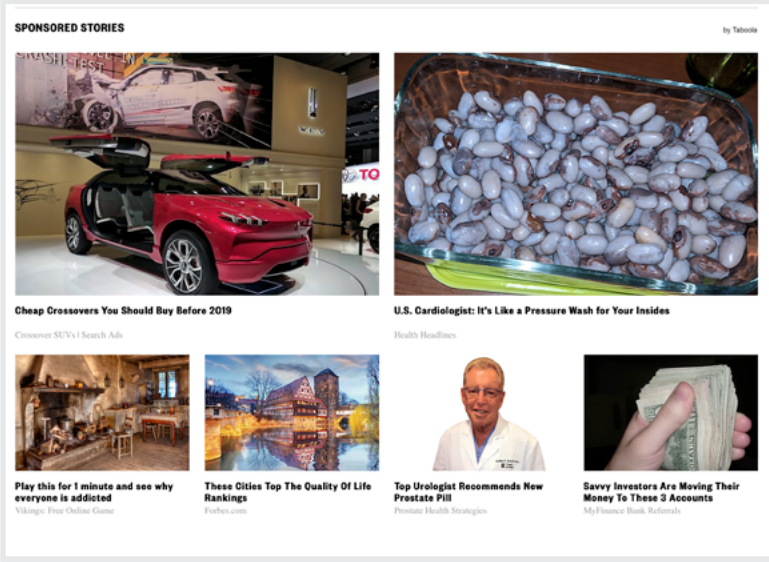
Analytics

We found Google Analytics on 64.2% of sites, with other services from Google having coverage on around 80% of all sites. Scorecard Research trails behind at 18.7%, but that still reflects a presence on 1,322 different websites.

Analytics tools and "marketing insight" scripts, both of which collect substantial quantities of data about a site's visitors, are some of the most popular scripts on the web. Many sites, including Variety, ZDNet and UK tabloid the Sun, have more than 30 different analytics and marketing trackers included on every page load.

Advertising

The proliferation of analytics is only beaten by advertising trackers. We found Google's DoubleClick ads on 54.4% of the top sites. Criteo, one of the web's most popular providers of retargeting ads, was found on 14.6%. That's why those same ads seem to follow you everywhere! Taboola, provider of the most hideous and recognizable clickbait, was found on 4% of the 7,000 most popular sites.



Which link is most tempting to click? What does that tell advertisers about you?

Core functionality provided by third parties

It always surprises me how many sites rely on third parties to provide critical site functionality. Of the top sites, 19% link directly to Google's Ajax API. It's also common to find core functionality, such as login forms and mailing lists, hosted by third parties. We found 5.8% of sites use the Bootstrap CDN, 5.2% use Optimizely for A/B testing content, and 5.3% of sites use YouTube for hosting video content.

26. *http://smashi.ng/trackers*

Enhancements

It's more common to rely on third-party sites for enhancements — the nice-to-have additions such as web fonts, performance-enhancing scripts, and social sharing buttons. Ubiquitous use of Facebook's Like buttons and tracking pixel have resulted in Facebook's presence on 30.3% of sites, effectively letting Facebook follow you around the web. A whopping 28.9% of the top sites use Google Fonts, widening Google's reach further still.

Content

Amazon's AWS is used on 12.2% of the top sites as a content delivery network (CDN). Third-party CDNs are incredibly popular, with most images and other media seemingly hosted in this way. Many sites use their own subdomains or short domains to host content too.

Can track, might track

Not every third-party resource on a site is tracking you. But most resources *can* track you. And even if they don't track you now, they could do so in the future: if they need to make more money, or if they get bought by a company that wants to track you.

It'd be easy to tell you to stop using technology lest you become addicted to its engaging features, and have your privacy invaded entirely. A lot of articles are written chastising poor stupid technology addicts who can't control their screen time. This makes me angry because it's blaming the victim. It's not our fault we've become hooked on products that are deliberately designed to addict us. Technology does not have to be designed this way.

How we can change it all

We shouldn't keep tracking people because "everybody else is doing it." We need to make significant changes. Not just personally, or inside our organizations, but on a much bigger scale.

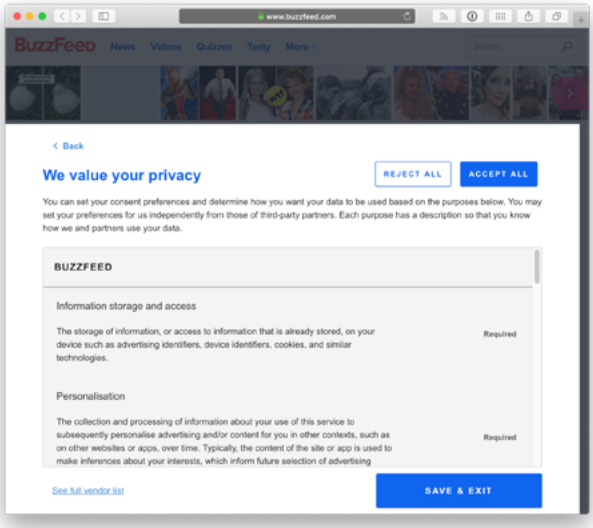
Regulation

While bad publicity can hurt an unethical business, a corporation is answerable only to its shareholders and the law. Its shareholders don't necessarily value our rights over their financial gain, but the law is supposed to protect us from business malpractice.

In May 2018, the General Data Protection Regulation (GDPR) came into effect in the European Union (EU). This regulation doesn't just apply to sites served from the EU, but sites whose visitors are inside the EU. Heather Burns wrote a thorough article covering the role of developers in meeting the requirements of the GDPR.[27]

Much of the GDPR was deliberately designed to reduce tracking by requiring explicit consent for the collection of data about individuals. For now, this has resulted in awful dark-pattern consent modals that make the options confusing and hard to understand; the lists of trackers are long and boring, and the buttons make it unclear what would help protect your privacy. And that's if you can be bothered to read them in the first place. Most people will just click whatever button they can to get to the content they want, and the websites have designed the interfaces to encourage this behavior.

27. *http://smashi.ng/gdprcompliance*



BuzzFeed's consent dialog discourages you from selecting "Reject All" by using low-contrast styles compared with the other buttons.

In time, the regulators will likely fine these bad practices. This, alongside public shaming and detrimental publicity, will hopefully make nefarious business models riskier and less attractive to tech entrepreneurs looking to make big money from fast growth. We've all heard tales of developers who made a cool million when their company got its "exit" by going public on the stock market, or was bought by a bigger corporation. It shouldn't be aspirational to profit from products that exploit their users.

California is also leading the way with the US's strictest regulation on collecting people's data.[28] It goes into effect in 2020. Google, Facebook, Verizon, Comcast and AT&T opposed the bill and lobbied against it, even though it is still not as strict or specific as the EU's GDPR. Lobbying against consumer rights isn't anything new: Facebook, Google and Twitter spent $30m lobbying in Washington in 2017.[29]

Better business models

Businesses don't have to wait for regulation to make them do the right thing. We need alternative business models that don't rely on tracking, just as we need new funding models that don't rely on exponential growth and exits.

The current alternative to the "free" (as in zero-dollar) surveillance-based enticements of Silicon Valley is the old-school business model of paying for a product or service. This might be a one-time payment for an app, a subscription to a service, or through patronage. While this might be a good short-term solution, it does still mean that privacy is a thing you can buy only if you can afford it. And simply paying for a service doesn't guarantee you will not be tracked either.

As the surveillance-based web has become vital social infrastructure, we must start to consider funding ethical alternatives to it from the commons. We can and should use taxes to incentivize ethical digital infrastructure for the common good. This is not to say that governments should own and control these alternatives, but that they should be funded from the common reserves in a manner that guarantees they remain part of the commons if and when they're successful. We need imagination to think beyond

28. *http://smashi.ng/privacylaw*
29. *http://smashi.ng/siliconpolitics*

today's centralized, surveillance-based web to a sustainable and ethical internet, inclusive to all and outside the control of authoritarian governments and greedy businesses.

Questioning our own ethics

As an employee, you are unlikely to be able to change the business model of your employer. You may not have the privilege to easily find another job that can support your family, or to start your own business. But next time you look for a new job, favor the employers who are ethical. Make sure you know how a business makes its money.

It's not hard for us to minimize the tracking on the sites we build. Self-host your analytics, rather than sharing the data with a big corporation. Shun third-party services in favor of first-party options. Remove that twentieth marketing script, because only one person ever checked out its "insights" and they've forgotten their password anyway.

Small steps are better than no steps. But we won't reform technology unless we push hard.

We are the gatekeepers of the web. Nothing gets deployed to the server without us knowing about it, and we need to take responsibility. We must start thinking beyond the web to a future where we don't have to be trusted because we don't have access to people's information in the first place. We shouldn't be collecting people's information. We should be empowering them to own their

> **We shouldn't be collecting people's information. We should be empowering them to own their information and control what they choose to share.**

information and control what they choose to share. We should be building ethical alternatives.

The world in 2019 feels like we are already losing many of our rights. When so much of our industry operates in an unethical manner, and our industry underpins so much global infrastructure, it will take a lot of work to change the status quo.

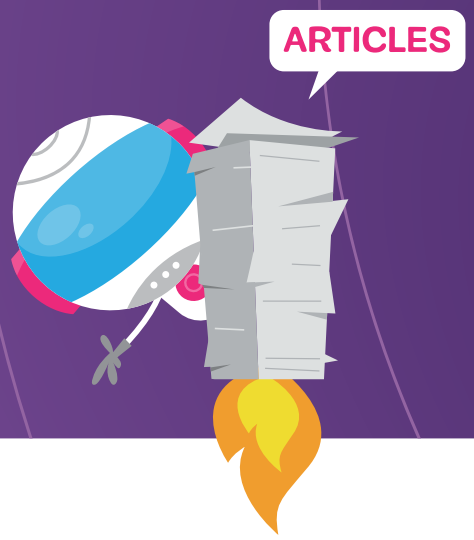
But it will be worthwhile. It's more fun to work on projects where you benefit the humans around you. It's enjoyable to write code and copy, and produce prototypes and pixels when you feel assured you're not harming people. And this is an area where you can truly effect change.

ABOUT THE AUTHOR

Laura Kalbag

Laura Kalbag is the co-founder of Ind.ie, a tiny not-for-profit working for social justice in the digital age. At Ind.ie, Laura follows the Ethical Design Manifesto, and works on a web privacy tool called Better Blocker. Laura is also the author of *Accessibility For Everyone* from A Book Apart. laurakalbag.com

The Smashing Universe revolves around you



THE SMASHING UNIVERSE IS FULL OF WAYS FOR you to learn — articles, printed books, eBooks, Smashing TV, conferences, and our print magazine, because different people learn differently. But whichever you choose, you can be sure that it's written, edited, and produced with love. Learning should be a pleasure.

Our Smashing Books aren't lumps of information thrown on cheap paper. They're professionally designed by Markus, and then given a quality hardcover with stitched binding and a ribbon page marker, because we want our books to be like your websites: a great user experience. And, of course, if you buy a print book, you get the digital book for free.

We don't farm out Smashing Conferences to an events company. Amanda, Charis and Mariona are part of our Smashing Family, so they spend their time working crafting personal, inclusive and valuable events for all of us to become better professionals. No fluff, no fillers, no multi-track experience and no large hotel halls. Instead, speakers and topics curated by Vitaly, sessions and hands-on workshops in a friendly, inspiring and exciting setting. They are the conferences that we would want to attend or speak at.

You like articles? We've published over 2,000 articles over our 11 years, covering web development from A to Z. Well, A to W; we haven't found any subjects beginning with X, Y or Z.

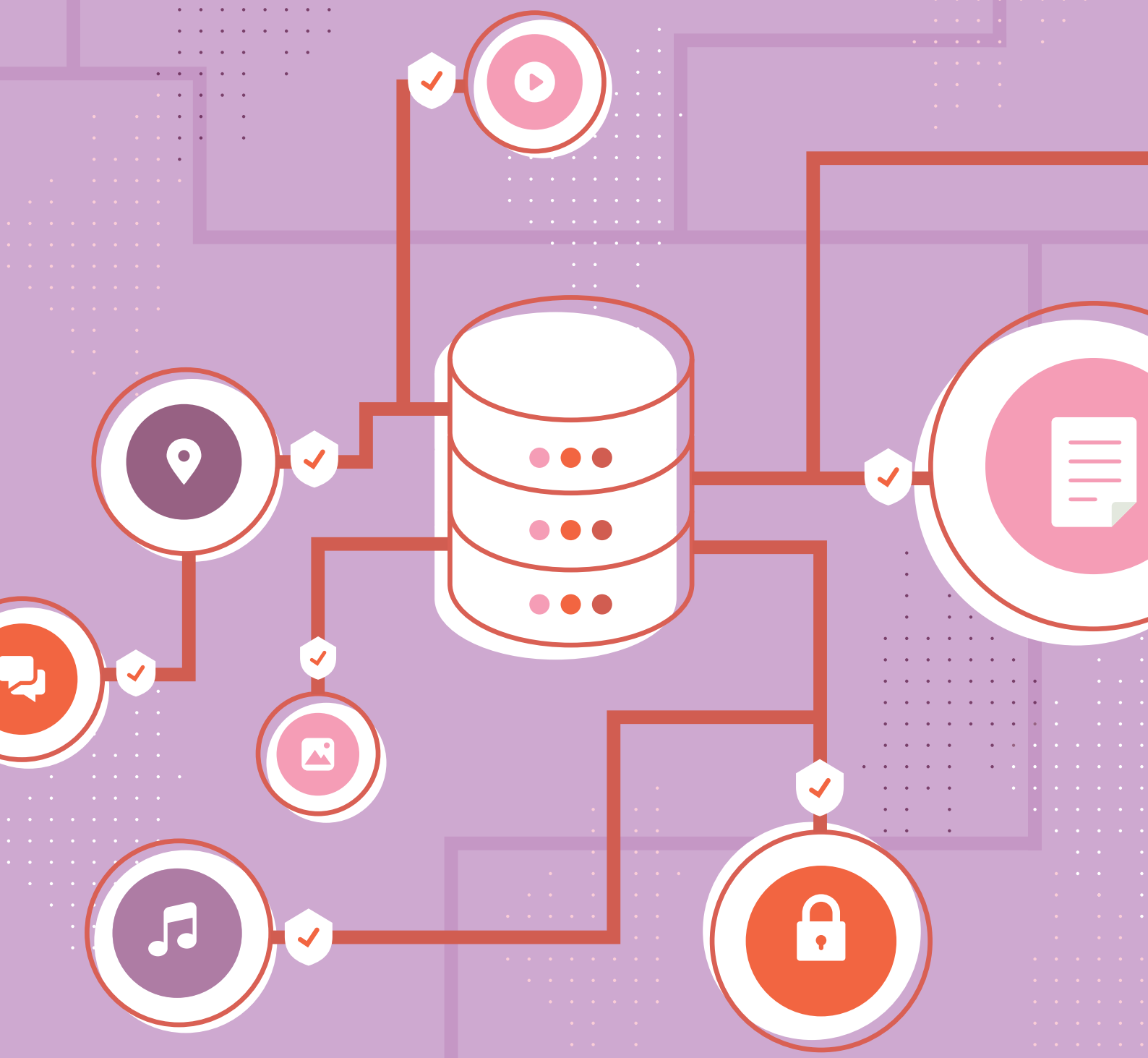
They're all free to read, carefully tech-edited, and each of the authors is paid for their remarkable contribution. Work matters and deserves to be rewarded.

Smashing Membership is a transparent and affordable way to get access to all our resources. From between $3 and $9 a month *(cancel anytime!)*, you get access to eBooks, discounts on conferences, and Smashing TV — live video education with a chance to ask questions of the speaker.

We love the web. We seek best practices to ensure we all craft accessible, performant sites the right way, so the web remains as inclusive, international and diverse as our readers, authors and team.

Quieting Disquiet

by Stuart Langridge



IN 2012, TARGET, THE AMERICAN DISCOUNT STORE, PUT together a list of 25 products that when purchased together indicate that the purchasing woman is likely pregnant. Then they mailed out coupons for baby products to prospective mothers... and the father of one of them stormed into his local Target and demanded to see the manager. "My daughter got this in the mail!" he said. "She's still in high school, and you're sending her coupons for baby clothes and cribs? Are you trying to encourage her to get pregnant?" And then a couple of days later he apologized profusely when she revealed that she was, in fact, pregnant.[30]

Women are less likely to be shown ads for high-paying jobs, found Carnegie Mellon academics in a 2015 study.[31]

Facebook has patented technology to use a loan applicant's social network to assess whether they are a good credit risk, meaning that your social media friends might be making it harder for you to get a loan.[32]

Collecting data became the new big thing: the way digital services made money, a rich vein of gold funding whole swathes of the new economy. Data is the new oil: the world's most valuable resource, we were told. Like all gold rushes, it was untapped ground and the first people in there made a ton of money; but also like all gold rushes, there's a crash coming. And the crash, for data collection, is people finding out about it.

In the space of only a couple of years, we've gone from mainstream unawareness of personal data to a public sense of disquiet about what's done with it, how much it's collected, and what happens next.

5

30. *http://smashi.ng/loanpatent*
31. *http://smashi.ng/concerns*
32. *http://smashi.ng/creepyline*

Today, if the word "data" shows up in a headline, it's normally followed by "breach," and this is starting to filter into the consciousness of people who use these services, not just our industry which builds them. In a world where the heads of large digital companies are called to testify in front of government, and the front pages of the newspapers report on Cambridge Analytica for days at a time, this discussion is out there in the world and not just inside our communities. The idea that Facebook does strange things you don't know about with your data is part of current mainstream discourse. Tinfoil hats are now a fashion item.

There's a part in almost all the Sherlock Holmes stories where Holmes makes an amazing deduction about his client, based on his analysis of seemingly innocuous details about them. The "Sherlock scan" and the deductions are almost his defining characteristic. But flip the story around, and look at it from the client's point of view. They are surprised and disquieted and alarmed: how does this man, who knows nothing about me, know so much about me?

We are an industry who rightly talk about user experience a great deal, who elevate UX above most of the other things we need to do.

> **Your data collection is creepy when you use it to derive things you weren't told and shouldn't know.**

But what happens when surprising deductions are made from innocent data is that the client is alarmed and concerned, while Sherlock looks clever at their expense. That's not the experience users want. They do not like it.

Half of all Americans have avoided doing some basic thing online because they fear the unknown uses their data will be put to.[33] A huge majority of people are not comfortable with the sale of their data to third parties in exchange for speed or convenience or product range.[34]

Your data collection is creepy when you use it to derive things you weren't told and shouldn't know. That's what Target did. It's what Sherlock Holmes did. And it's what rather a lot of digital businesses routinely do.

But that's a rather one-sided view of things. Nobody is collecting data because they want their users to feel disquieted and concerned. There are genuine uses for this. It is important to get feedback, to work out what your users do (and when and how), to refine and improve your

33. *http://smashi.ng/target*
34. *http://smashi.ng/jobads*

product based on how it's being used, to iterate and A/B test, and gather information about the types of people you've got, and the types that you want.

A stern refusal to countenance any data gathering at all, or to insist that all data is end-to-end encrypted and not available to the people who build the service, essentially makes for worse services.

It's optimizing for the wrong thing; if the data you need to make your thing better is outlawed, then we just make more outlaws. There needs to be a balance: respecting people's right to feel comfortable about what's being done with their data, but also respecting a company's goals of making the product better so those people actually get the improvements they want. It's possible to build privacy-respecting services without them having to be privacy-focused services.

So what do we do about it?

One way may be to consider the uses the collected data is put to. The thing which concerns people is how much is known about them, and how much confidential information can be deduced about them from that. Whereas, what at least some companies want is to make aggregate judgements about their user base: how many people are in this age bracket as opposed to that, or are home-owners as opposed to not, or are married, or European, or pet owners — aggregate information about whole sections of their user community, not specific information about individual people. And if you only need aggregate information, and you therefore only collect aggregate information, then the amount you compromise people's privacy is considerably reduced.

In the 1960s, social scientists were faced with a problem. They wanted to ask people questions about sensitive issues (Have you used illegal drugs? Evaded paying taxes?) but respondents were understandably reluctant to go on record confessing to things that were criminal. The approach they invented was called the randomized response method. It allows people to give answers while being able to credibly claim, if later confronted with the answer they gave, that they were not being truthful and, therefore, were not incriminated.

How it works is like this. Ask a respondent a question, such as, "Have you smoked marijuana?" Before they answer, they secretly flip a coin. If the coin comes up heads, they answer truthfully. If tails, they lie; they give the incorrect answer, so someone who has smoked says they have not.

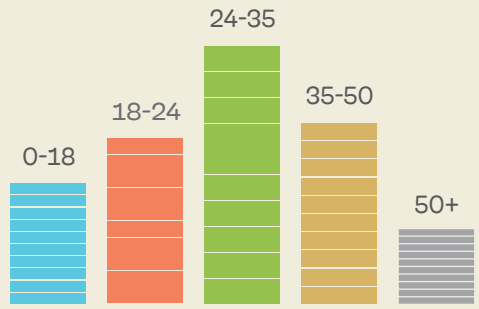
After all the respondents in the survey have answered in this way, the responses are tabulated. After some simple mathematical manipulation, the results obtained will be correct; if 25% of participants have smoked marijuana then the manipulated results will indeed show that 25% of people have done so.

But any one person's answer is unreliable: if a respondent is confronted with having answered yes to this incriminating question, they can credibly say that their answer was actually no, but their secret coin flip was tails.

Any given answer is not incriminating, but the aggregate results of the survey are still correct and so correct conclusions can be drawn from them.

This isn't limited to coin flips. Imagine you'd like to collect data on the age of your users to get a sense of demographic spread. You'd like to classify them into age brackets: 0–18, 18–24, 24–35, 35–50, and 50+. The truth is that you have more users in the 24–35 bracket, fewer in 18–24 and 35–50, and fewest in 0–18 and 50+. This is the data you'd like to know, but you want to collect it without compromising your users.

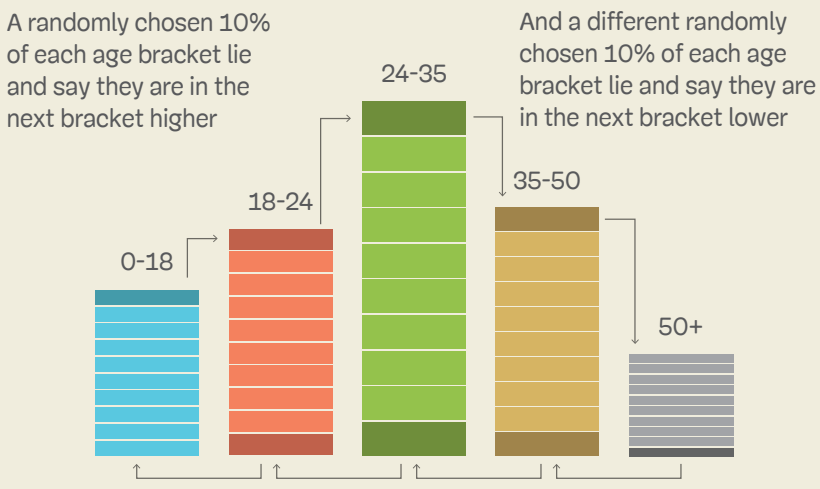
To work with a randomized response and protect your users' privacy, when your app reports the user's entered age back to your servers, have it lie 20% of the time. 80% of reports report the truth; 10% lie and say they're in the age bracket below (so an actual age of 27 is reported as 18–24, not 24–35); and 10% lie and say they're in the age bracket above.



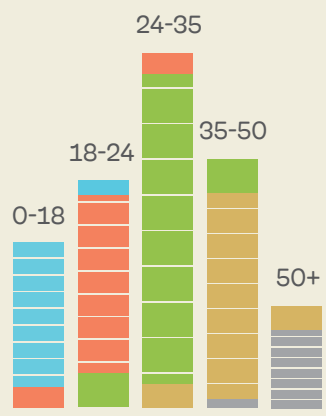
Actual age distribution of the user base

So, as above, a given user's report is unreliable; even if you wanted to keep this data about your community, you won't know whether a specific user was part of the 20% and so lied. But, remarkably, even given that, the results reported to you are roughly still the truth. Your reported results still show that you have most users in the 24–35 bucket and fewest in 0–18 and 50+.

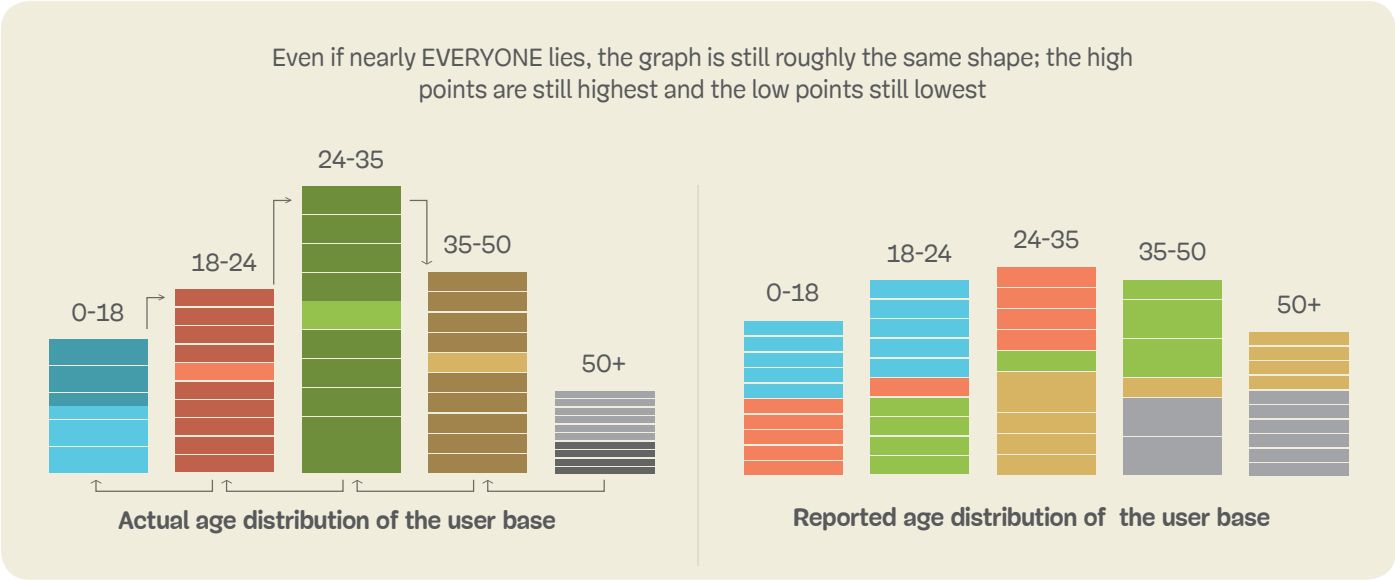
Even more interestingly, that 20% figure isn't fixed. Even if almost every response is a lie — so nobody's data is accurate at all — the results you collect



Actual age distribution of the user base



Reported age distribution of the user base



still show a similar-shaped graph: there are still most users in the 24–35 bucket and fewest in the outlying groups.

The results of your data-gathering get more and more inaccurate as you increase the number of users who lie about their results — raising the percentage of deliberately incorrect answers tends to flatten the results graph, making peaks shallower and troughs taller — but the overall conclusions you can draw are still correct. This allows you to tune the results based on the needs both of your data science team and your user community; dial-up user privacy at the expense of accurate predictions, or trade off that privacy to get more accuracy in your demographic data. Exactly where the sweet spot lies depends on the product, the business, and the customer relationship, but now that can be an explicit decision taken by you rather than the previous situation of choosing between collecting everything and collecting nothing.

This approach to data gathering requires almost no code changes at all, which makes it easy to implement. After collecting the data ready to send back to the server, for each data point move it, with a 20% chance. It can be as simple as:

```
CONST R = MATH.RANDOM();
IF (R <= 0.1 && DATA.AGE_BRACKET > 0) {
    DATA.AGE_BRACKET -= 1;
} ELSE IF (R >= 0.9 && DATA.AGE_BRACKET < 4) {
    DATA.AGE_BRACKET += 1;
}
```

That is, just change the data collected on the client side or in the app, before reporting it. Nobody — not you, not even the users themselves — knows whether their data were changed; that's what protects their confidentiality. And this is the simplest and most tractable approach; there are many subtler and more detailed techniques that are better, once people come to demand that their data is protected when collected.

And this becomes a thing you can trade on. It's been said before that attempting to make privacy the selling point of your app doesn't work, that it only attracts people for whom privacy is their only concern. This is true. But the increasing sense of disquiet in the mainstream means that it can be a selling point, along with all your existing work on the user experience and delighting your people.

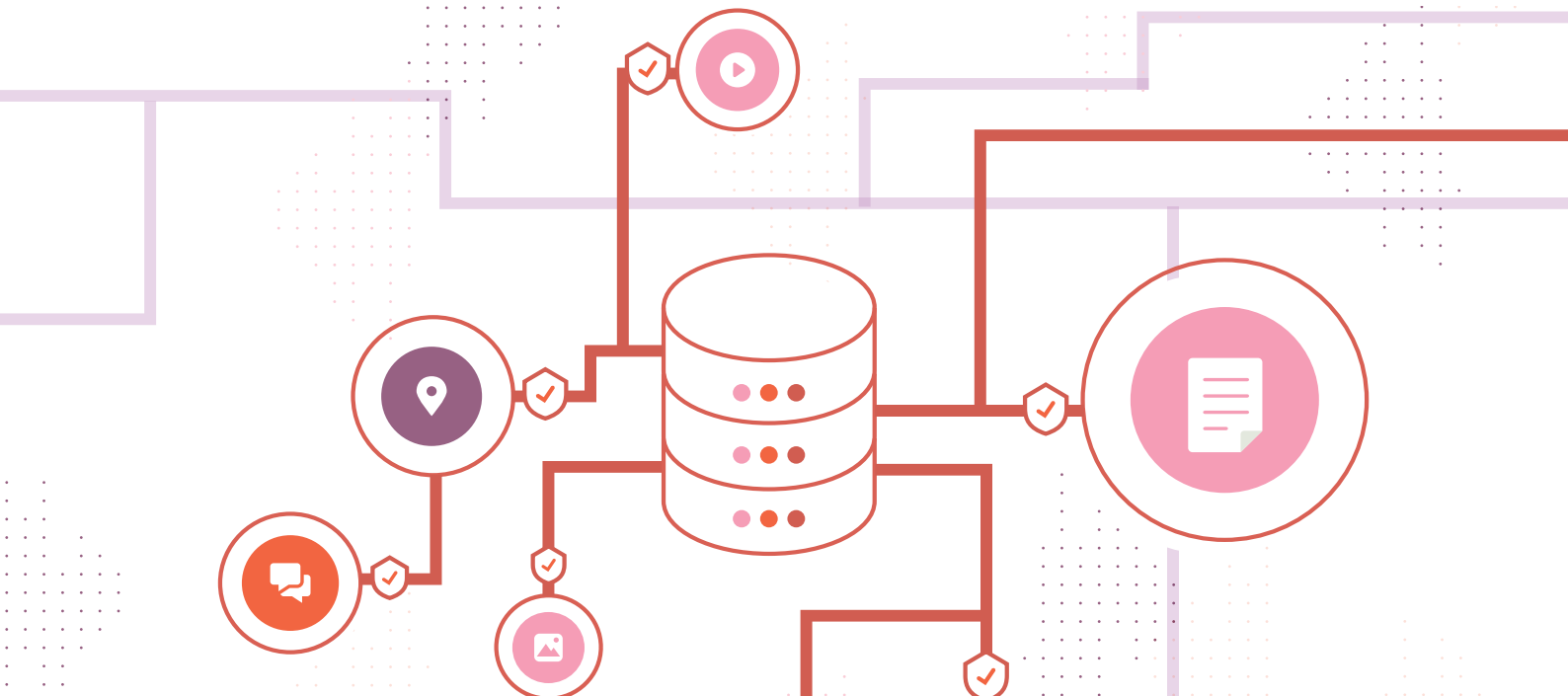
The big names, at least those who don't have a business model critically reliant on user data, already know this. WhatsApp makes something of a big deal about its encryption, and Apple is talking more and more about on-device security and differential privacy. This is something that can make you a thing apart from and ahead of your competition, who won't or can't compete on this playing field. And if you take a lead here and your competition follows along behind, then we've made a world where everything is as it was before, except user confidentiality is protected — and that's a great thing. Our industry concentrates so hard on the user experience, on delighting people, on fitting into their lives in newly obvious ways; we should and can take the lead on this. Show people that their choices are more than just opting out or giving up. That they can have the world at their fingertips and don't have to sell themselves to do it. Let's fix this.

ABOUT THE AUTHOR

Stuart Langridge

Stuart is a consultant CTO and software architect to startups and small firms on strategy, custom development, and building things. Code and writings are to be found at kryogenix.org and @sil on Twitter; Stuart himself is mostly to be found hidden behind a huge pile of books that still need reading.

kryogenix.org



Advertising Is Not The Problem

by Cennydd Bowles

WHEN IT'S TIME FOR Q&A, THERE'S often someone who sticks their hand in the air and says, "Hi, yes, this ethical design stuff is all very nice, but until we abandon the ad-funded business model, surely it's a waste of time?" I have seen the beast, and its name is surveillance capitalism. Then, with a faint smile, they trot out that beloved line—"If you aren't paying for the product, you're the product being sold"—and people nod alertly in recognition of an adept outflanking maneuver; yes, I thought that too, let's focus on the real problem.

These people are usually surprised to hear me disagree. However, it's hard in a short sound bite to elaborate on where I feel their thinking has come up short. It needs a more detailed take. Here it is.

Like it or not—and there are indeed plenty of reasons not to like it—advertising is the only proven way to bring affordable technology to the world. We can thank the public purse for much of the early work: the infrastructure of the internet, the web itself, and email all grew as a result of public, scientific, or military endeavor. But now that the invisible hand of capitalism has become a fist around our throats, there's little global appetite to throw more public funding behind technology. We now look to the market as a provider, while the dreams of a volunteer economy have also faded away. Early cyberutopians hoped the web's citizens would trade favors for favors, contributing to the world's knowledge through sheer generosity, and transcending the need for petty commerce. This model survives perhaps in Wikipedia and a handful of niche services, which scrape by on donated time and the occasional holiday campaign, but is otherwise long forgotten.

So someone had to pay, and advertisers were happy to step into the void. Their funding helped to unleash some remarkable innovation: ad-funded models have brought the world the search engine, the messaging client, the photo-sharing service, the social network—imperfect technologies, to be sure, but technologies we could hardly imagine going without today.

The model of consumer-funded technology—pay up front and own the thing outright—is the one that critics of advertising tend to harken back to.

But ours is a different era to that of pre-internet software, with its oversized boxes stacked high on retail shelves, three-figure price tags for spreadsheet software, thick manuals, and stacks of floppy disks. Consumer sales are still the best model for hardware, which has high capital and marginal costs: in other words, since it costs a lot to make a smartphone, and roughly twice as much to make two, it's natural to push that cost onto the consumer. But asking consumers to pay for software now seems like a doomed strategy. Unlike hardware, software has almost no marginal cost: once you've made the thing, you can duplicate and scale it to millions easily. The public seems to have decided to stop stumping up the cash, as evidenced by plummeting prices in the app stores. Increasingly, the only software you can sell is business software; even these are moving from up-front purchase to annual subscriptions.

Abandoning ad-funded models would require us to somehow reverse this trend and convince customers to pay for software again. This seems unlikely. But there's a more fundamental problem: a return to consumer-funded software would also drag us back to the bad old days of technology being a plaything of the rich. Even $5–10 a month (the usual bracket suggested by the "just let me pay to get rid of ads" campaigners) is a hefty slice of a worker's monthly salary in most of the world. The insinuation that technology is only ethical if paid for by the user is, therefore, an insinuation that the poor, that developing nations, that children — the very people who could benefit most from technology — don't deserve ethical technology. Consumer-funded software is a luxury good, a retreat into inequality, a betrayal of the democratizing promise of the connected age.

> **So someone had to pay, and advertisers were happy to step into the void. Their funding helped to unleash some remarkable innovation: ad-funded models have brought the world the search engine, the messaging client, the photo-sharing service, the social network—imperfect technologies, to be sure, but technologies we could hardly imagine going without today.**

Social software amplifies the exclusion. As Metcalfe's law tells us, the effect of a network is proportional to the square of the number of users on it. We've seen this play out firsthand with the slew of anti-Facebook and anti-Twitter competitor social networks: techies flock to them, but no one else cares, and they quickly rot away to nothing. A social network with a membership

fee will by its nature exclude most of the world, and be worthless as a result: a snobbish haven for rich techies. As Anil Dash says, you can't start the revolution from the country club.

A freemium model might seem like a reasonable compromise: could we support mainstream users with advertising, achieving the huge reach that social networks and search engines need, and also offer people the opportunity to opt out of advertising by paying a subscription? Unfortunately, the message is again worrying: if we claim advertising is unethical, it looks like we're saying it's fine for poor people to suffer it, while the rich get to opt out. There's also a compelling economic refutation. Advertisers want to sell to rich users: in marketing departments the world over, red circles highlight affluent market segments. Wealthy customers bring in the most profit, spend most freely, and are often significant influencers within their personal networks. A platform that lets its richest users opt out of advertising will soon find that advertisers suddenly lose interest: if they can't reach their most lucrative market, why bother?

Advertisers will either flee the platform or pay significantly lower rates, and the entire model collapses inwards. It's no accident that even premium publishers and cable TV services still subject their readers and viewers to commercials.

Given the flaws and impracticalities of the alternatives, ad-funded technology is here to stay. However, the critics do have a point: there are some troubling aspects to today's technologies. To see these clearly, we must be precise, and recognize tracking as something distinct from advertising. This isn't a pedantic separation: it hinges on fundamental ethical issues such as visibility and consent.

Advertising — showing adverts, be they text, audio, video, in a product — can certainly be annoying. We've all hunted for a tiny close icon as a pop-over smears its way across the screen; we've all rolled our eyes at an unskippable pre-roll. But beyond these minor dark-pattern inconveniences, advertising is part of an agreed contract: I get some useful functionality, in exchange for seeing some adverts. For this reason, I think ad-blockers are generally unethical — you're trying to wriggle out of your end of a prearranged, consensual deal, contravening the promise-keeping that forms an important part of a healthy society.

> **Advertisers do benefit from tracking. But so does every other company, regardless of the business model.**

Tracking is a far bigger ethical problem. Its mechanisms are hidden, and its dangers multiplied with aggregation. Information that is harmless in isolation can become painfully revealing when spliced with other datasets. Many of us are happy to give up our locations, credit card histories, and heart rates, but anyone with the power to combine all three could easily assemble evidence of serious medical issues, or perhaps an affair. Tracking typically happens at the fringes

of consent. Perhaps some lawyer approved a line buried in the terms of service; even GDPR pop-ups are often designed in a way that makes exercising one's data protection rights a tedious process. It's easy to argue that the social contract between provider and user has already been broken, meaning there's a stronger ethical case for tracker-blockers than for adblockers. We can see blocking trackers as an act of self-defence more than of promise-breaking.

There's a counterargument here, though. Isn't tracking required by advertising? Companies only want to show ads to people who will act on them, so surely any company that wants to maximize ad revenue is incentivized to target and track their users? This is absolutely true: advertisers do benefit from tracking. But so does every other company, regardless of the business model.

User data has become a vital commodity for the workings of modern tech. Even the business press has realized this, blurting on demand an alarming new cliché: data is the new oil. This metaphor is at least admirably honest: businesses see personal data as a raw material, a natural resource to be burned for profit. Every tech business today is therefore desperate to extract value from user data; to see this as just the domain of advertisers is a sadly antiquated perspective.

One use case is analytics. In thrall to metrics, objectives and key results, and experimentation, firms both inside and outside the tech sector are eager to measure the successes and failures of their strategies. This thirst for analytics, for dashboards and bar charts, requires tracking.

But the main growth industry for user data is AI. Machine-learning systems require vast sets of training data to create models, which are then let loose on future datasets. AI is central to thousands of ambitious business strategies, but comes with a large strategic hurdle: a competent AI will need to consume an enormous amount of training data, which companies either have to gather themselves, or buy in somehow.

User experience also plays an important role. Data isn't just needed for training these systems; it's central to how they are used. A user can by all means choose to withhold personal data from, say, a voice assistant, but this reticence will come at a price: the system will be a pain to use, and will never improve by knowing the user better. A bot with amnesia will quickly gather dust; opt out of your bank's new security tech and you're thrown back into the old world of unwieldy passwords and code generators.

It's a fundamental mistake, therefore, to argue that the advertising industry is responsible for the abuses of user tracking. Today, all businesses benefit from tracking. It makes no difference whether you are paying or not; you are the product either way.

This is, admittedly, an unhappy conclusion, but it at least stresses that technologists are all responsible for respecting users' personal data and minimizing the harms of tracking. How then do we protect users, if tracking is so ubiquitous, so fundamentally necessitated by all forms of modern digital capitalism?

> **The tech industry has become a target for both political wings, and today it seems almost inevitable that regulation is on the way.**

At a bare minimum, technologists must be aware of and adhere to their local data protection laws, or perhaps stronger ones, such as the EU's GDPR. But a more thorough response is to adopt privacy-by-design approaches that put user consent right at the heart of tracking, and to resist dark patterns that capture more data at the expense of precious user trust.

Designers, in particular, have an important role to play. For years, the UX field has treated data as complexity, something best hidden underneath the hood of a system, something that users have no business understanding. It's time to let users interrogate systems to see how their data is being collected, processed, and transmitted. Privacy specialists sometimes call this transparency, but I think this is precisely the wrong framing. Something transparent cannot be seen. Better instead that we materialize data, giving form to something previously spectral. If we shift data flows into the visible spectrum, people will be able to better understand what is happening inside their technologies, and start to finally trust that their devices are acting in their own interests.

This change may, sadly, be too much for the industry to do of its own volition; others may have to force our hand. The tech industry has become a target for both political wings, and today it seems almost inevitable that regulation is on the way. This will include new data protection rules (where, of course, the EU is ahead of the game), but is likely to stretch to bot self-disclosure, rules on disclosing ad funding, and limits on persuasive systems. I predict these new rules will hit within 5–10 years; if we truly believe in respecting our users' privacy and autonomy, we can hardly argue that more oversight isn't deserved.

ABOUT THE AUTHOR

Cennydd Bowles

Cennydd Bowles is a London-based designer and writer with fifteen years of experience advising clients including Twitter, Ford, Cisco, and the BBC. His focus today is the ethics of emerging technology. He has lectured on the topic at Facebook, Stanford University, and Google, and is a sought-after speaker at technology and design events worldwide. His second book, *Future Ethics*, was published in 2018. cennydd.com

The world is a miracle. So are you.

Thanks for being smashing.

The web is wonderfully diverse and unpredictable because of the wonderfully diverse people shaping it. Behind each lifeless dot in our analytics stats is an actual person, so every single dot matters.

Humility and kindness are all too rare on the web. But each of us deserves to be respected and valued, and how companies treat our data is fundamental to achieving that. So the first edition of our new printed magazine is dedicated to an issue very close to our hearts: ethics and privacy.

Feel free to pass this issue of the magazine to your friends, colleagues, neighbors and total strangers. We hope that every time you flip through it, you'll find some pointers worth discussing over a fire chat, or techniques applicable to your work.

Of course, the print edition is, and always will be, free for Smashing Members. Without them, this magazine wouldn't be able to exist. So thank you from the very bottom of our hearts — and here's one for the next issues! ❤️

— *Vitaly*