2025–2030 0.0¢ PAID WITH PERSONAL DATA • EXPERIMENTAL EDITION • First public release • VOLUME 1

THE 100 WORST TERMS AND CONDITIONS YOU'VE ALREADY ACCEPTED

BANNED IN 13 C
BANNED
FOR CONCERNED CITIZENS

A RED ZONE MANUAL FOR BIG TECH FINE PRINT

DECLASSIFIED

THE 100 WORST TERMS AND CONDITIONS YOU'VE ALREADY ACCEPTED

Authorship
Text, Curation, Prompts, and Methodology by Sérgio Tavares. Content Written and/or Augmented by OpenAI Deep Search, a system by OpenAI LP. Vintage Illustrations Created by MidJourney

Publisher
Geist Media
Publisher Identifier: 978-952-7588

Publication Details
Publication Date: Spring 2025
ISBN: 978-952-7588-03-1
Language: English
Total Pages: 108
Publishing Format: Electronic (PDF)
Dimensions: 140 mm x 210 mm
Approx. File Size: 45 MB

ADDITIONAL NOTES

Methodology
This book merges original research and commentary with AI-assisted text generation. All sections have been carefully reviewed and edited by Sérgio Tavares for accuracy and clarity.

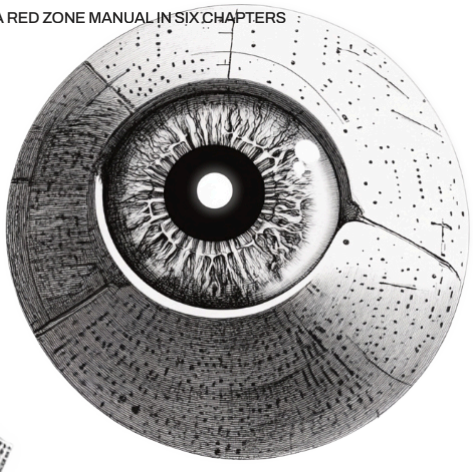
Creative Process
The vintage-style illustrations were generated using MidJourney, aligning with the book's retrospective take on legal documents and user agreements.

Acknowledgments
Many thanks to the OpenAI Deep Search team for supplying the language model support, to Geist Media for bringing this digital publication to life, and to all the contributors who provided insights on user rights and data privacy.

Disclaimer
This text is provided for informational and educational purposes. It should not be considered legal advice. Always consult official Terms and Conditions from each service for the most up-to-date policies and any legal questions pertaining to your circumstances.

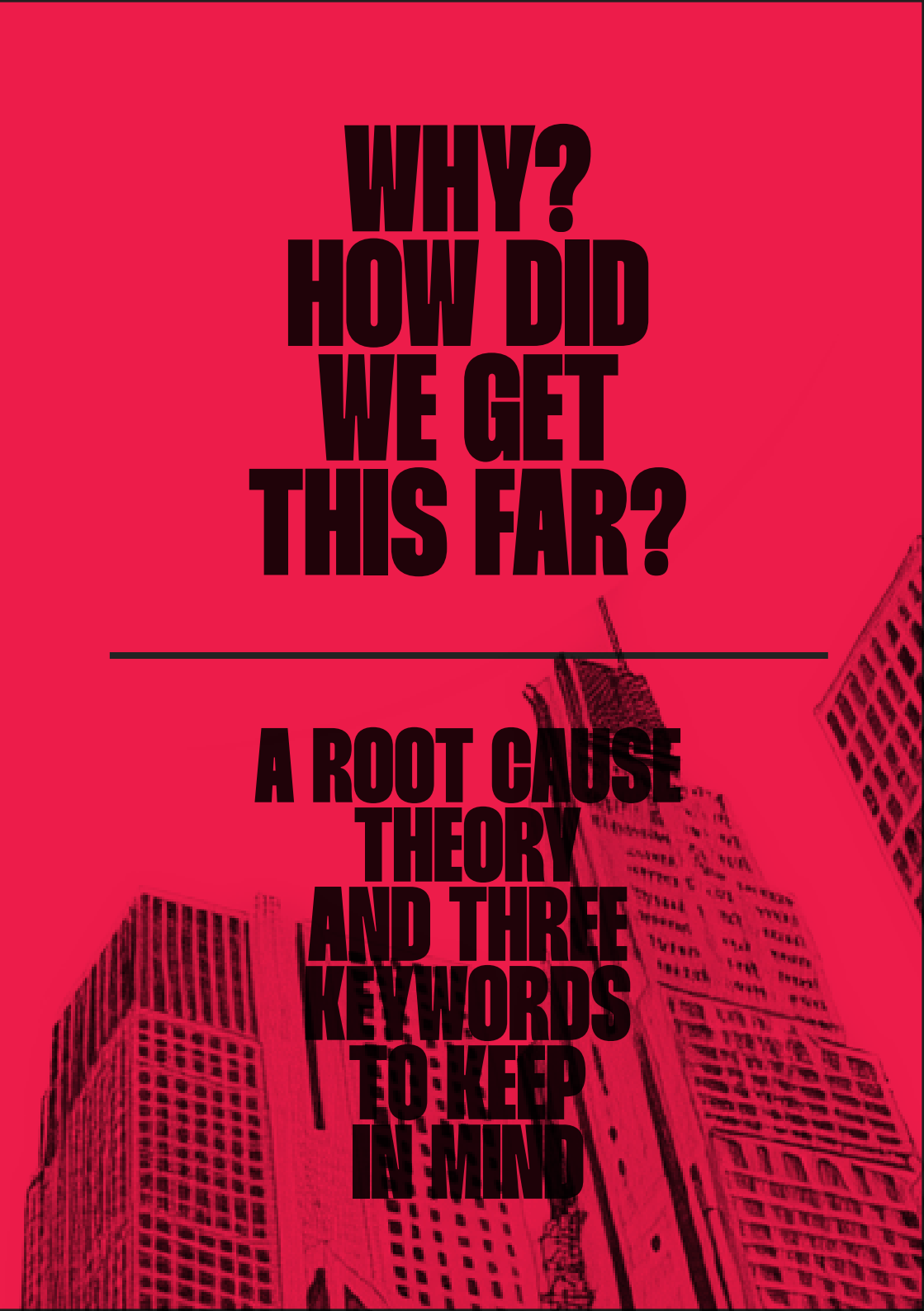
THE 100 WORST TERMS AND CONDITIONS YOU'VE ALREADY ACCEPTED

A RED ZONE MANUAL IN SIX CHAPTERS



WHY? HOW DID WE GET THIS FAR?

A ROOT CAUSE THEORY AND THREE KEYWORDS TO KEEP IN MIND



WE HAVE LOST THE CAPACITY TO QUESTION THE ROOT CAUSE OF THE PROBLEM.

HOW DID WE GET HERE?

Behind “I agree” there is a number of decisions asked from us which are deliberately obscured. Us, the users, are kept in a state of perpetual unknowing. This sounds as conspiratorial as real. Seems like we blinked, and here we are. This Red Zone Manual serves as a field guide to this subtly alarming present. It points out to a more alarming future—where something feels distinctly off, but not enough to scream.

The pursuit of frictionless user experience (idealized as a form of liberation through design), paradoxically erodes the its exact purpose. In the effort to reduce cognitive load and eliminate barriers, interaction designers have often designed away the opportunity for critical reflection.

As Seymour (2020) argues, friction, far from being a flaw, is what allows experience to emerge through conscious attention and choice. This echoes the work of Lukoff et al. (2021), who proposes that well-placed friction can support empowerment, accountability, and even justice. Instead, many of today’s digital systems push users toward “thoughtless interaction,” where agency is quietly automated away.

This is not a passive process. A growing body of work on dark patterns—a term coined by Harry Brignull and expanded upon in large-scale studies like Mathur et al. (2021)—demonstrates how interface design is often

crafted to manipulate rather than guide. These design patterns are not accidental; they are systematic efforts to steer user behavior in ways that serve corporate interests, from pre-checked boxes to deceptive interface hierarchies. In these environments, consent becomes less an act of understanding and more a performance of inevitability. Trouble is, eCommerce dark patterns are easy to spot. But when every "I agree" choice is opaque, it becomes hard to understand we are in the dark.

Byung-Chul Han's work offers a crucial philosophical lens on this landscape. In The Transparency Society, he argues that under the banner of positivity—efficiency, convenience, transparency—we eliminate "negativity": doubt, slowness, resistance, reflection. And as Han suggests in The Disappearance of Rituals, the erosion of shared, meaningful acts (like informed consent) creates hollow performances of engagement—where clicking "I agree" carries the ritual form of consent, but none of its substance.

At the same time, the legal and regulatory framework that should protect user agency has been chronically outpaced. The agility of product updates, machine learning algorithms, and data-sharing partnerships routinely outstrip the cognitive and legal capacities of both users and oversight institutions. As Yeung (2021) warns, the emergent logic of algorithmic regulation creates a form of governance without legibility—where decisions are made, but understanding is postponed indefinitely. Calo (2020) further shows how behavioral science is weaponized in these environments, creating digital architectures that exploit attention and bypass rational deliberation. The result is a system in which regulators chase the tail of technological development, and users are left with only the illusion of control.

The triumvirate we propose—OPAQUE, OUTPACE, and PERFORM—defines the architecture of modern consent:

OPAQUE. Terms and conditions are designed to be unreadable and unreasonably complex. As Couldry and Mejias (2021) argue, the data economy thrives on a "coloniality of power," where complexity serves as both a barrier and a justification. Transparency becomes aesthetic rather than substantive.

OUTPACE. The pace of innovation ensures that by the time a user understands the implications of one system, the next one has already emerged. This is not a side effect; it is a strategic advantage.

PERFORM. Consent becomes a ritual. Bucher (2021) refers to the "algorithmic imaginary," in which users simulate understanding simply to keep interacting. In this world, clicking "I agree" is not about agency—it is about staying in the game.

This cycle feeds itself. What we encounter as individual decisions—whether to download an app or update software—are in fact systemic concessions, fragments of a broader surrender. Palfrey and Gasser remind us that even digital natives, immersed in the digital world from birth, are overwhelmed by its hidden complexity. If even the most fluent struggle to understand the systems they interact with daily, what hope do others have?

As Levy (2011) documented in In the Plex, the inner workings of platforms like Google are designed to be inscrutable—not just to users, but often even to regulators and developers themselves. The opacity is recursive.

We often assume that the worst cannot happen: that no harm will come from one more click, one more overlooked clause. And perhaps, on an individual scale, it won't. But systemically, the aggregated consequences of millions of such clicks are profound. We are building a digital infrastructure in which human agency is systematically deskilled.

YOU, THE USER ACCEPTING TERMS, IS NOT THE PROBLEM.

This is not about blaming users. It is about recognizing a design and legal culture that strategically disempowers. The normalization of data extraction, surveillance, and behavioral nudging is no longer a glitch in the system—it is the system.

The Red Zone Manual is not a guide for reading the fine print. It is a guide for understanding the forces that produce it—legal, psychological, aesthetic, and structural. If we cannot realistically ask everyone to read every clause, we must ask why such clauses exist in this form, and what systems of power they enable. In the end, the central question is not whether users are responsible for reading the Terms and Conditions, but whether the fine print they are agreeing to is so small it is not readable at all.

SOURCES

Brignull, Harry. Dark Patterns: Inside the Interfaces That Manipulate You. MIT Press, 2023.

Bucher, Taina. “The Algorithmic Imaginary: Exploring the Ordinary Affects of Facebook Algorithms.” Information, Communication & Society, vol. 24, no. 1, 2021, pp. 30–46.

Calo, Ryan. “Digital Market Manipulation.” The George Washington Law Review, vol. 82, no. 4, 2020, pp. 995–1051.

Couldry, Nick, and Ulises A. Mejias. The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism. Stanford University Press, 2021.

Ericson, Jonathan. “Reimagining the Role of Friction in Experience Design.” Journal of User Experience, vol. 17, no. 4, Aug. 2022, pp. 131–139. User Experience Professionals Association. http://uxpajournal.org.

Han, Byung-Chul. The Disappearance of Rituals: A Topology of the Present. Polity, 2020.

Han, Byung-Chul. The Transparency Society. Stanford University Press, 2015.

Han, Byung-Chul. Shanzhai: Deconstruction in Chinese. MIT Press, 2017.

Han, Byung-Chul, et al. The Agony of Eros. MIT Press, 2017.

Ito, Mizuko, et al. Hanging Out, Messing Around, and Geeking Out: Kids Living and Learning with New Media. MIT Press, 2019.

Levy, Steven. In the Plex: How Google Thinks, Works, and Shapes Our Lives. Simon & Schuster, 2011.

Lukoff, Kurt A., et al. “The False Binary of Frictionless and Disruptive Design: Rethinking Friction in HCI.” Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, ACM, 2021, pp. 1–15.

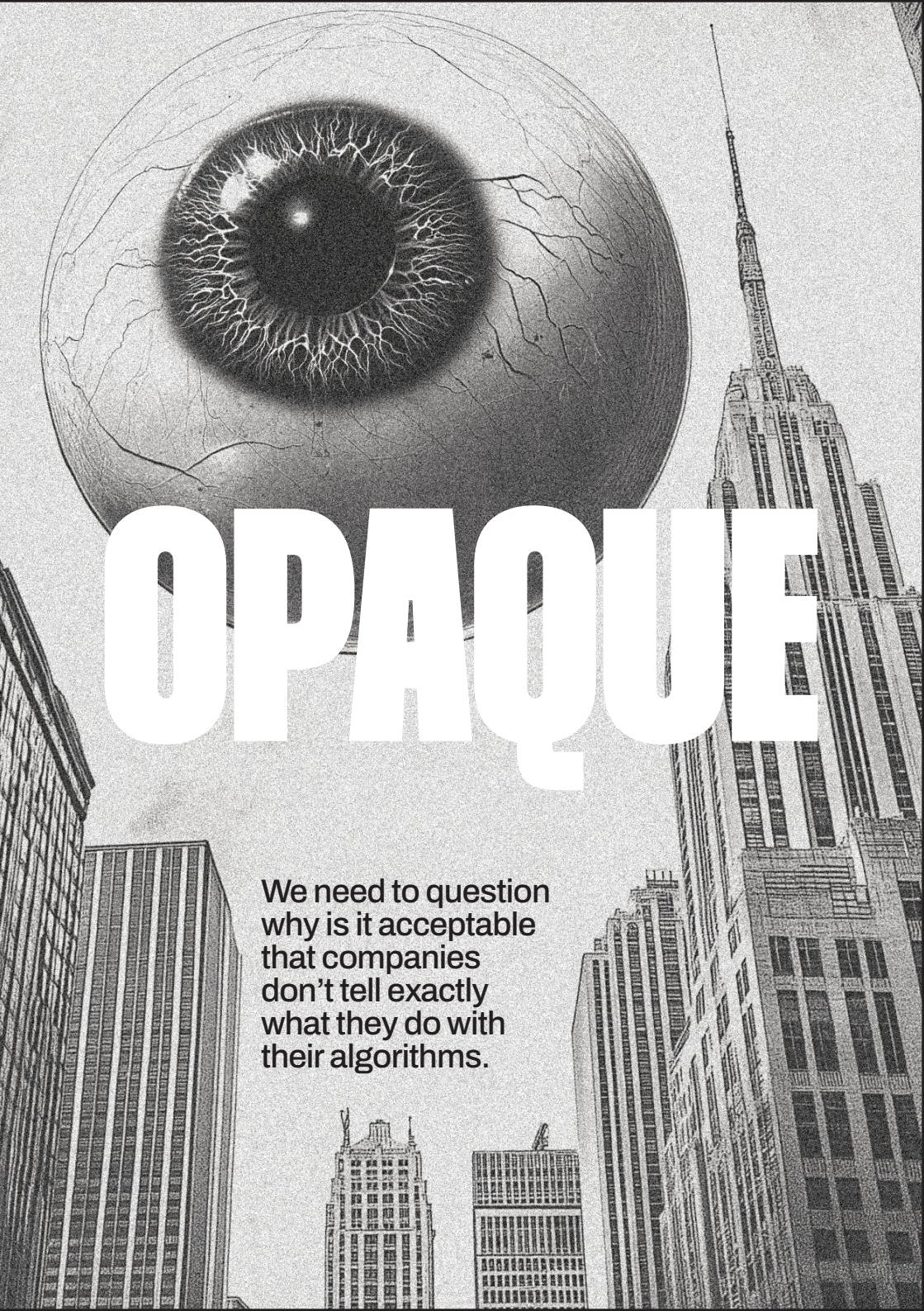
Mathur, Arunesh, et al. “Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites.” Communications of the ACM, vol. 64, no. 8, Aug. 2021, pp. 67–73.

Palfrey, John, and Urs Gasser. Born Digital: Understanding the First Generation of Digital Natives. Basic Books, 2008.

Seymour, Aaron. “In Praise of Inconvenience: Rethinking Frictionless Experience.” AMPS Proceedings Series 18.2: Experiential Design – Rethinking Relations between People, Objects and Environments, edited by Y. McLane and J. Pable, Florida State University, 2020, pp. 173–180.

Yeung, Karen. “Algorithmic Regulation: A Critical Interrogation.” Regulating Digital Futures, edited by Lilian Edwards, et al., Routledge, 2021, pp. 20–42.

Zuboff, Shoshana. “You Are Now Remotely Controlled.” The New York Times, 24 Jan. 2021, https://www.nytimes.com/2021/01/24/opinion/sunday/surveillance-technology.html.


OPAQUE
We need to question why is it acceptable that companies don't tell exactly what they do with their algorithms.

OPACITY IS THE GREAT ACCELERATOR

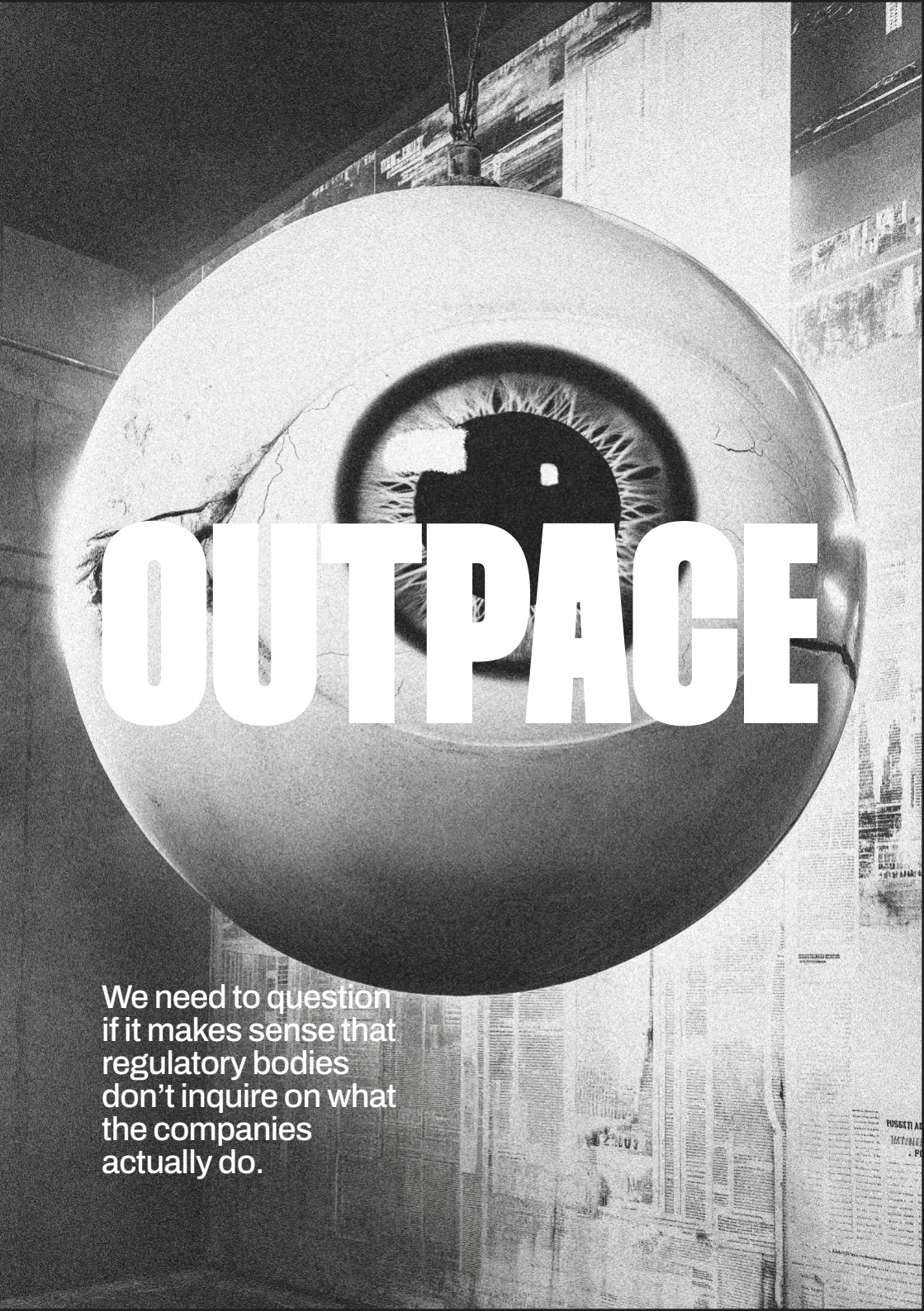
Companies using vague language and long agreements are just the tip of the iceberg when it comes to lack of transparency.

Widespread adoption of services make obscure practices normalized.

> We still don't know who are "the partners" that get our data from Facebook, nor how YouTube recommends—or monetizes—videos.

We don't question them when we join the services, the practice becomes standard, and the cycle restarts.

But these don't operate alone. All subsequent reasons listed here are interconnected to enable the practice.

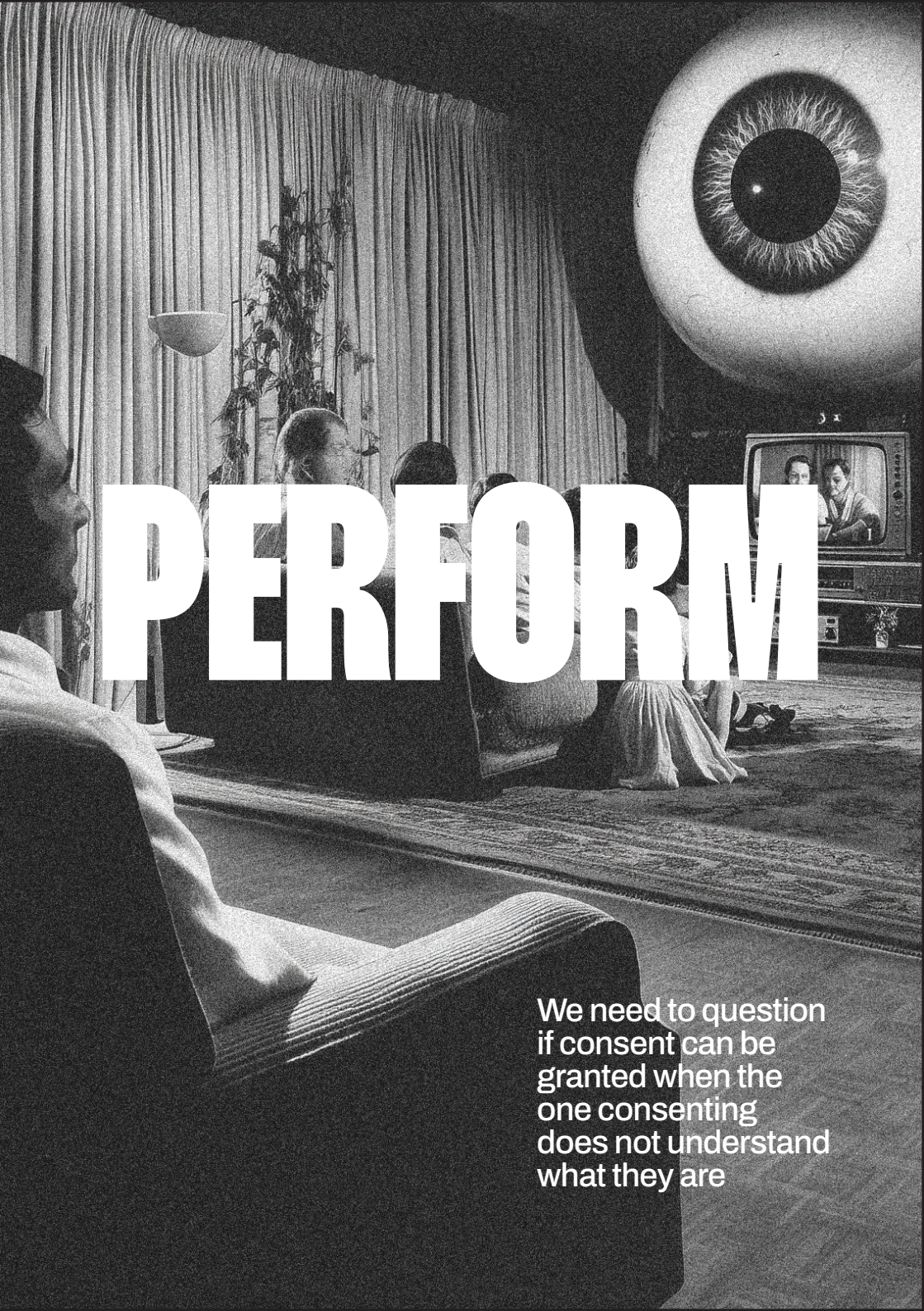

OUTPACE
We need to question if it makes sense that regulatory bodies don’t inquire on what the companies actually do.

INTELLECTUAL OUTPACING

The tech moves faster than law can even name it. Capturing the regulatory bodies (lawmakers, regulatory agencies) is a lot about keeping the terms and conditions obscure, so the ones in power cannot understand how the services work.

The perfect example are Zuckerberg's hearings in the American Senate in 2018 (and numerous other similar occasions), in which lawmakers asked shamefully naïve questions — a power imbalance that keeps all companies with comfortable margins to operate as they please.

The knowledge gap is a strategy, enabled and sustained by the original opacity of how companies work and what they disclaim in their agreement terms.


PERFORM
We need to question if consent can be granted when the one consenting does not understand what they are

CONSENT IS A PERFORMANCE

We live in a “click to consent” society. The market doesn't need to coerce when it can seduce. Our culture rewards speed and simplicity. Clicking “Agree” is the smoothest path.

This isn’t the end user’s fault.

> The end user trusts that accepting those terms is OK, because some regulatory body and market competition balance has checked those out as “safe”.

However, when big tech operates as an oligarchy, the opaque practices benefits them all and deepens the problem Companies move faster, and break more things.

The intellectual outpace of regulatory bodies comes back into play — it benefits the industry as a whole, and is therefore conveniently maintained by the first point raised here, the acceleration provided by opacity.

I

FIVE BEHAVIORAL PATTERNS THAT WOULD MAKE A SOCIOPATH BLUSH

FROM INVASIVE DATA PRACTICES TO UNILATERAL CONTENT — THIS IS THE DEEP DIVE.

Technology companies have built vast empires on user data and engagement – and their Terms and Conditions reflect that imbalance.

We analyzed the fine print of industry giants like Meta, Apple, Amazon, Netflix, Google, Microsoft, TikTok, Twitter (X), PayPal, Disney+, Uber, Airbnb, and others.

First, we distill 5 key problematic patterns that emerge across these contracts.

Then, we found about 100 risky clauses that erode consumer rights.

These range from invasive data practices and unilateral content ownership to forced arbitration agreements and sweeping liability waivers.

> We highlight 20 egregious excerpts (with detailed evaluations), 30 highly questionable excerpts, and 50 somewhat questionable clauses.

Many of these clauses share common themes. In fact, across these industries, there are five key patterns of problematic terms that repeatedly emerge. We'll start from there.


1.

SNEAKY PRIVACY LOOPHOLES

Companies routinely reserve the right to surveil users – gathering personal data, messages, location, biometrics – often under broad auspices of “improving service” or “safety.” Facebook scanning Messenger chats, TikTok collecting faceprints, Google analyzing your emails, and Disney tracking your viewing habits are all manifestations of a surveillance economy. The terms create legal cover for extensive data harvesting, often without clear, granular consent. Users effectively agree to be watched. This erosion of privacy is typically buried in dense language, meaning people seldom realize just how much monitoring they’ve consented to.


2.

LOSS OF USER AGENCY & CONTENT CONTROL

From content licenses that never expire to unilateral term changes, T&Cs strip users of control. Once you upload content – be it a photo, a video, a review – nearly every platform grants itself an expansive license to use or alter that content however it wishes. Users also lose control through clauses allowing services to remove content or suspend accounts at will. Unilateral change clauses (like Facebook's "we can change terms anytime") mean users aren't truly consenting to a fixed contract but an ever-shifting one. The upshot: you're not really in control of your digital identity or even the rules you play by – the company is.


3.

VAGUE LANGUAGE TO AVOID TRANSPARENCY

Many terms are opaque, using catch-all phrases like “objectionable content” or “at our sole discretion.” This vagueness gives companies maximum flexibility but leaves users in the dark about enforcement or expectations. PayPal’s now-notorious $2,500 fine clause was a masterclass in obscurity until it made headlines. Likewise, phrases such as “information you provide… and other information we collect” fold in a lot of potential data without spelling it out. Non-users being tracked by cookies, or data being shared with undisclosed partners, fall into this transparency gap. When terms hide key practices in legalese or fail to spell out consequences clearly, users effectively cannot give informed consent – undermining the premise of a mutual agreement.

FORCED ARBITRATION & LEGAL RIGHTS RESTRICTIONS

An overwhelming pattern, especially in U.S. user agreements, is the curtailment of legal remedies. The waiver of class-action lawsuits and mandate of private arbitration appear in Microsoft, Amazon, Google, Airbnb, and more. These clauses fundamentally tip the scales by preventing users from banding together or using the public court system in a dispute. By accepting the service, users often unwittingly sign away their right to sue in court or participate in a collective lawsuit – one of the strongest tools consumers have (for example, in fighting hidden fees or discriminatory practices). The result is that corporate misconduct, if it occurs, faces less risk of large-scale accountability via the justice system.


5.

EXCESSIVE PROFILING

Many T&Cs now explicitly confirm that user data will be used for behavioral profiling, advertising, and even AI training. Whether it's Amazon noting voice recordings might be analyzed, or X (Twitter) feeding your tweets to an AI, the trend is that any and all user behavior is fair game to feed algorithms. Some services link across platforms – e.g., Facebook can combine Instagram and WhatsApp data – creating super-profiles. The terms legitimize this by obtaining a broad consent for "personalized experience" or "service improvement," phrases that sound user-friendly but permit sweeping data fusion. The rise of generative AI adds a new dimension: user content can directly enrich AI models (as X now states). This category of clauses accelerates the creep of data usage beyond what users reasonably expect, raising not just privacy issues but questions of compensation (your data helps build a product that you may later be sold).

(The fine print reveals a consistent story: the services we love come at a hidden cost to our rights. These contracts are written by corporations to protect themselves first and foremost – often at the expense of user privacy, control, and recourse. While it's unrealistic to avoid all these platforms, being aware of these terms is the first step. Regulators and user advocates are increasingly scrutinizing such clauses, pushing for clearer language and fairer practices. Until then, remember that every time we check that "I agree" box, we may be signing away more than we realize – and it's worth understanding what we're giving up.)

II

TWENTY TERMS STRAIGHT OUT OF A BLACK MIRROR EPISODE

facebook

We reserve the right, at our sole discretion, to change, modify, add, or delete portions of these Terms of Use at any time without further notice… Your continued use of the Service… after any such changes constitutes your acceptance of the new Terms of Use. It is your responsibility to regularly check the Site to determine if there have been changes."

FACEBOOK'S ONE-SIDED TERMS CHANGE

Facebook can alter its rules whenever it wants, and the onus is on you to keep track. This unilateral change clause means users can wake up to new obligations or fewer rights without direct warning. It's a classic "take it or leave it" approach that strips users of any say in the relationship.

By submitting User Content… you hereby grant us an unconditional, irrevocable, non-exclusive, royalty-free, fully transferable, perpetual worldwide license to use, modify, adapt, reproduce, make derivative works of, publish, transmit, and/or distribute… your User Content in any format and on any platform, now known or hereinafter invented.”

TIKTOK’S PERPETUAL LICENSE TO YOUR CONTENT

TikTok users technically own their videos, but this clause gives TikTok free rein forever to do anything it wants with your creations. The license is perpetual and irrevocable, so deleting a video doesn’t fully retract TikTok’s rights. Essentially, you hand TikTok a blank check to exploit your content globally without payment.

By submitting, posting or displaying Content… you grant us a broad license… You agree that this license includes the right for us to analyze text and other information you provide and to… improve the Services, including… training our machine learning and artificial intelligence models… without any compensation paid to you.”

X (TWITTER) WILL FEED YOU TO A.I.

Under X’s newest terms, anything you tweet can be fed into Elon Musk’s AI projects. Even if you opt out of data sharing, the terms suggest X may ignore that and still use your words to train AI.

Violation of the Acceptable Use Policy… may subject you to damages, including liquidated damages of $2,500.00 USD per violation, which may be debited directly from your PayPal account(s)…”

PAYPAL’S $2,500 “MISINFO” FINE (LIQUIDATED DAMAGES)

This unprecedented use of user-generated content blurs the line between social media and surveillance, effectively conscripting users into AI development without consent or pay.

In an infamous update (later said to be “in error”), PayPal claimed the right to take $2,500 from users’ accounts for each policy violation, including what PayPal deems “misinformation”. This staggering penalty, decided at PayPal’s “sole discretion,” sparked outrage. It illustrates how a financial service can assert punitive control over user funds with vague justification – a severe erosion of financial agency and free expression.

Uber

"Uber… is not liable for damages or losses arising from any transaction or relationship between you and a driver… Our total liability to you… shall not exceed five hundred euros (€500)."

UBER'S LIABILITY CAP AT €500

When you use Uber, the company virtually washes its hands of anything that happens between you and the driver. If an Uber driver causes harm or an accident, Uber's terms say the company isn't responsible for those damages. In fact, even if Uber is at fault, they cap their liability at €500 in these terms. For perspective, serious injuries or losses could cost orders of magnitude more – but Uber preemptively limits what it might owe you, leaving riders (or courts) to fight that cap.

The Microsoft Services Agreement contains binding arbitration and class action waiver terms that apply to U.S. residents. You and we agree to submit disputes to a neutral arbitrator and not to sue in court… Please see Section 15 for details."

FORCED ARBITRATION & CLASS ACTION WAIVER

Microsoft's blanket services contract (covering Xbox, Skype, OneDrive, etc.) pushes users out of the public court system. By agreeing, you waive the right to a jury trial or to join any class-action lawsuit. Any dispute must go to private arbitration – a process often seen as favoring companies – making it harder for users to band together or seek meaningful legal remedy against Microsoft.

Meta

We collect the content, communications and other information you provide… including when you… message or communicate with others." And as CEO Mark Zuckerberg has confirmed, Messenger conversations are scanned by automated systems (and flagged content is reviewed by moderators).

META (FACEBOOK/INSTAGRAM) MONITORS AND READS YOUR MESSAGES

Many users assume private chats are off-limits, but Facebook's terms and practices say otherwise. Anything you send through Facebook or Instagram can be analyzed. Ostensibly this is for safety (e.g. malware and child protection scans), but it's done without individualized consent. It's a reminder that "private" platforms are not so private – the company is always listening.

We may collect biometric identifiers and biometric information as defined under U.S. laws, such as faceprints and voiceprints, from your User Content. Where required by law, we will seek any required permissions from you prior to any such collection."

TIKTOK'S BIOMETRIC DATA GRAB

TikTok's U.S. privacy policy quietly added this clause allowing it to gather unique biometric data from videos. The wording is vague – it doesn't explain why it needs your faceprint, how it defines a "faceprint," or in which states it would even ask permission. Essentially, by using TikTok you may be handing over your facial and voice data, fueling concerns about invasive profiling and who ultimately accesses this sensitive info.

amazon

If you do post content or submit material, and unless we indicate otherwise, you grant Amazon a nonexclusive, royalty-free, perpetual, irrevocable, and fully sublicensable right to use, reproduce, modify, adapt, publish, translate, create derivative works from, distribute, and display such content throughout the world in any media."

AMAZON'S LICENSE TO USE EVERYTHING YOU POST

Every product review, comment, or photo you share on Amazon becomes Amazon's to utilize forever. They can, for example, take your five-star review of a blender and plaster it on marketing materials or partner sites without asking or paying you. This expansive license even survives if you delete your post. It's an example of how companies turn user-generated content into a free asset bank.

Amazon reserves the right to refuse service, terminate accounts, terminate your rights to use Amazon Services, remove or edit content, or cancel orders in its sole discretion."

AMAZON'S SECRET ACCOUNT KILL SWITCH

In plain terms, Amazon can ban you or nix your orders at any time for any reason (or no stated reason). If Amazon suspects you violated something or just finds your account "commercially unviable," it can shut you out. Customers have reported accounts closed with gift card balances lost or Prime memberships voided without clear explanation. This clause underscores that your access to hundreds or thousands of dollars in digital purchases lives at Amazon's mercy.

Google

Our automated systems analyze your content (including emails) to provide you personally relevant product features, such as customized search results, tailored advertising, and spam and malware detection. This analysis occurs as the content is sent, received, and when it is stored."

GOOGLE SCANS YOUR EMAIL FOR ADS & INFO

Google's Gmail terms openly acknowledge that everything that flows through your Gmail inbox is scanned by algorithms. That's how you might see an ad for sneakers after emailing a friend about running. While Google positions this as delivering convenient features, it's effectively deep surveillance of private correspondence for profit. Notably, Google has faced lawsuits over this practice, but it remains baked into their service model.

Google

When you upload or otherwise submit content to our Services, you give Google (and those we work with) a worldwide license to use, host, store, reproduce, modify, create derivative works… communicate, publish, publicly perform, publicly display and distribute such content."

GOOGLE'S ALL-ENCOMPASSING CONTENT LICENSE

This sweeping clause (unchanged in Google's terms for years) means any file you put on Google Drive, any photo on Google Photos, or video on YouTube grants Google a broad license to exploit that content. Google argues it's just so their systems can display or process your data as intended. Still, the language is so broad ("in any and all media… now known or later developed") that it understandably spooks users – it sounds like you're signing away rights to everything you ever store with Google.

You are responsible for backing up… any important documents, images or other content that you store via the Service. Apple shall use reasonable skill and due care in providing the Service, but Apple does not guarantee or warrant that any content you may store or access through the Service will not be subject to inadvertent damage, corruption or loss."

APPLE'S NO WARRANTY ON ICLOUD DATA SAFETY

Apple's iCloud Terms bluntly tell users: don't trust us with your only copy of anything. If photos or files you keep in iCloud disappear or get corrupted, Apple takes no responsibility. They place the entire risk on the user. This lack of accountability – essentially "if we lose your stuff, that's on you" – is jarring given Apple markets iCloud for safely storing life's memories. It's a reminder to always have your own backups, as even a trillion-dollar company won't compensate you for lost data.

The Disney+ privacy terms allows tracking what you watch, when, and on which device, and sharing those details across the Walt Disney family of companies and advertisers. Disney collects information about your interactions with our content, which can be used to target ads on Hulu, ESPN+ or other Disney services you use.

DISNEY+ TRACKING AND SHARING YOUR WATCH HABITS

While not a single quotable line, Disney's overall terms paint a picture of cross-platform surveillance. Stream a Marvel movie on Disney+ and your viewing data can ripple out to inform what merchandise or theme park offer you see elsewhere. The lack of a clear opt-out and the broad sharing among affiliates means using Disney+ can quietly feed an entertainment empire with personal behavioral data.

NETFLIX

Hidden in (U.S.) Netflix's Terms is a section compelling arbitration for disputes and waiving the right to trial by jury or to participate in class actions. A 2019 version states "you and Netflix agree that any dispute… will be resolved by binding arbitration," and that no class lawsuits are allowed.

NETFLIX'S NO DAY IN COURT CLAUSE

Binge-watching your favorite show comes packaged with a legal gotcha: if Netflix overcharges you or breaches your privacy, you've agreed not to sue in a real court. Like many companies, Netflix pushes users into private arbitration, a move that shields the company from large-scale legal accountability (such as class-action suits over a price hike or a data breach). It's a heavy-handed legal maneuver for a simple streaming subscription.

Airbnb is not responsible for any damage or harm resulting from your interactions with Hosts or other users of the service." (Airbnb's terms also specify that hosts and guests contract directly with each other, and any problems are between them.)

AIRBNB WAIVES LIABILITY FOR GUEST–HOST INTERACTIONS

If a host's negligence causes you injury, or a guest trashes your property, Airbnb's stance is essentially "not our problem." They facilitate the booking but then step back and deny responsibility for what happens in the real-world transaction. That leaves users to pursue claims on their own. Combined with Airbnb's own forced arbitration clause (Section 22), it means Airbnb has built a lucrative business while legally distancing itself from the core risks involved in home rentals.

Any photo or video you post on Instagram comes with a license for them to "use, copy, modify, and distribute" your content globally, in connection with the service or promotion of it. Instagram's terms specify this includes placing ads next to your content or using your content to promote Instagram (for example, featuring your post in an Instagram advertisement).

INSTAGRAM CAN USE YOUR PHOTOS HOWEVER IT WANTS

Your vacation snapshots could inadvertently end up as part of Instagram's marketing machine. By using the app, you've okayed Meta to take your imagery and run with it for commercial purposes (though they don't claim ownership). This broad rights grab is why, periodically, artists or photographers rebel at how they must either accept Meta's terms or forgo the platform. It underscores the loss of control creators often face on social media.

Google

Google's Terms in the U.S. impose that "You must initiate any proceeding or action within one (1) year of the event giving rise to the dispute. Otherwise… you forever waive the right to pursue a claim."

GOOGLE'S 1-YEAR TIME LIMIT TO SUE

This clause is a sneaky way to short-circuit statutes of limitations that might normally be longer. If, say, you only discover two years later that Google misused your data or overcharged you, Google's terms say it's too late to seek redress – you've waived your rights by then. It's an obscure deadline that most users would never know about, effectively immunizing Google from older claims even if the law would have given you more time.

Uber

In the U.S., Uber's terms have included an arbitration agreement compelling individual arbitration for disputes and a clear waiver of any class-action rights. (Often phrased as: "By agreeing to these terms, you agree that you may bring claims only in your individual capacity, not as a plaintiff or class member in any class or representative action.")

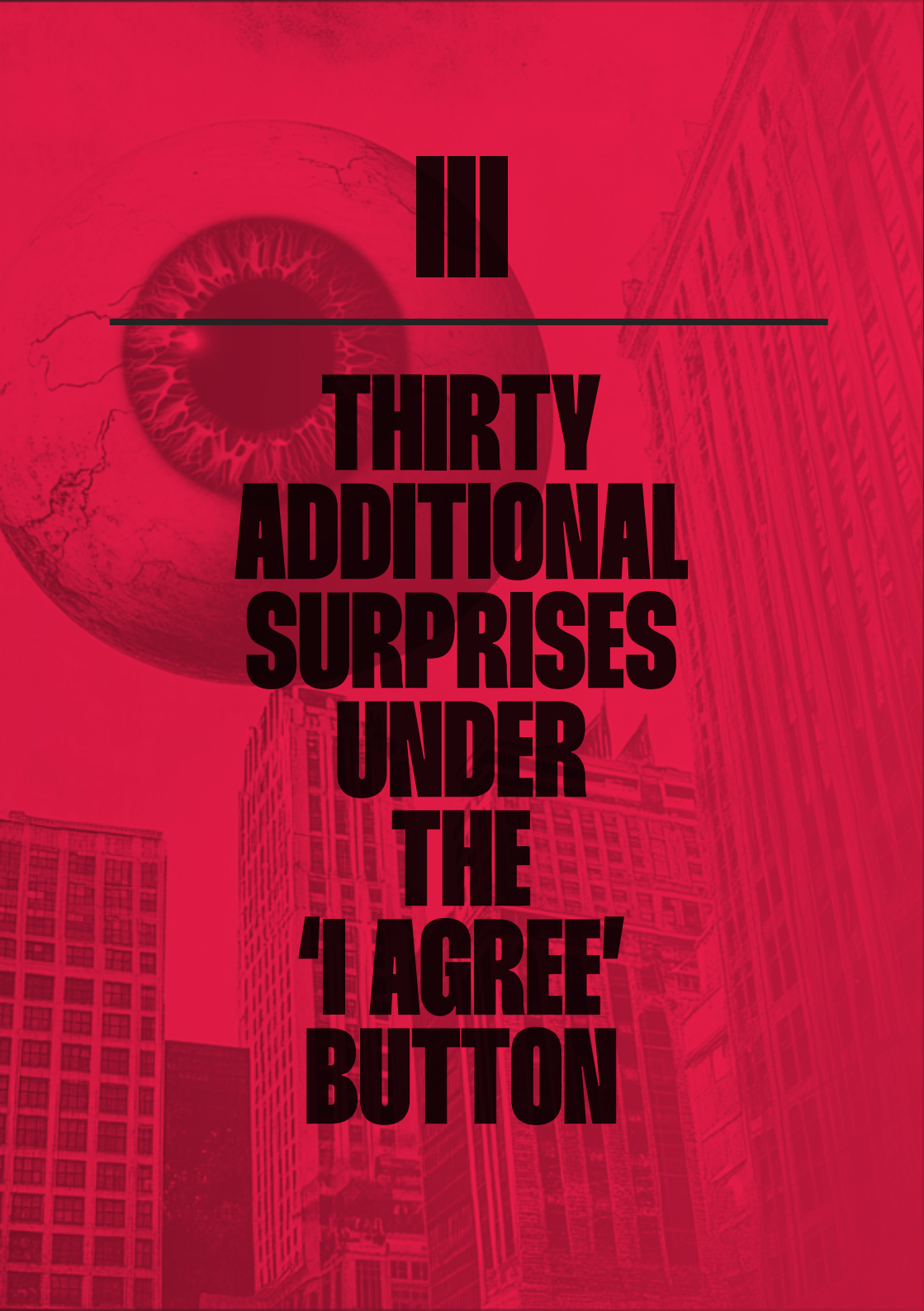
UBER'S ARBITRATION & NO CLASS ACTIONS (U.S. VERSION)

Much like other Silicon Valley giants, Uber shields itself via arbitration clauses. For riders or drivers, this means any legal claim – from a fare dispute to a serious safety incident – must be handled one-on-one, usually confidentially. By barring class actions, Uber prevents users from collectively addressing systemic issues (for example, a class-action over alleged racial discrimination in ride cancellations or widespread wage issues for drivers). It's a powerful deterrent against large-scale legal challenges.

PayPal's User Agreement spells out that if you violate their rules or they suspect fraud, they can put a hold on your funds for 180 days or more. In fact, for Acceptable Use Policy violations, PayPal states "the hold may remain in place longer than 180 days" and even that they might seize those funds as damages for the violation.

PAYPAL CAN FREEZE YOUR MONEY FOR 180+ DAYS

For small merchants or individuals, this is chilling. PayPal can unilaterally lock up your balance for half a year – essentially an interest-free loan of your money to PayPal – and there's little you can do. Many users have complained of sudden account freezes with cash trapped. The fact that PayPal also alludes to keeping the money (beyond just refunding customers) as "damages" for a violation shows how these terms skew heavily in PayPal's favor, acting as prosecutor, judge, and jury over your funds.



III

THIRTY ADDITIONAL SURPRISES UNDER THE 'I AGREE' BUTTON

Meta

You should know that, for technical reasons, content you delete may persist for a limited time in backup copies… and may continue to appear if you have shared it with others who have not deleted it."

META'S CONTENT DELETION ISN'T FINAL

When you "delete" a Facebook post or an Instagram photo, it's not truly gone. Meta keeps backup copies and if anyone else (friends, followers) saved or reshared it, your content lives on. This ambiguity around deletion means your data can linger indefinitely on company servers or on other users' pages – raising privacy concerns despite a user's intent to remove information.

By posting content, you waive any rights to prior inspection or approval of any marketing or promotional materials related to such content. You also waive any and all rights of privacy and publicity or any other rights of a similar nature in connection with your User Content."

INSTAGRAM'S WAIVER OF PERSONAL RIGHTS

Not only does Instagram get a license to your content, but you also give up rights to object to how they use it. They could feature your post in an ad; you've waived rights to claim it violates your privacy or uses your image without permission. For users, this means effectively surrendering say over how their name, likeness, and posts are used by the company in the future.

All disputes related to these Terms or the Services… will be brought exclusively in the U.S. District Court for the Northern District of Texas or state courts in Tarrant County, Texas, and you consent… waive any objection as to inconvenient forum… To the extent permitted by law, you also waive the right to participate as a plaintiff or class member in any class or representative action."

TWITTER'S CLASS ACTION BAN & TEXAS COURTS MANDATE

Twitter (X) not only bars class actions, it also dictates that if you sue them, you must go to their home turf in Texas. For a user in, say, California or New York, that is burdensome. This forum-selection combined with a class-action waiver means Twitter/X is minimizing its legal exposure: no large collective lawsuits and all cases handled in a potentially more company-favorable jurisdiction.

Though TikTok's Terms differ by region, in the U.S. they push disputes to arbitration (as indicated by the "Dispute Resolution" section) and bar class actions in a similar fashion to others.

TIKTOK'S ARBITRATION FOR U.S. USERS

TikTok's youthful user base might not realize that by dancing along on the app, they've agreed to serious legal constraints. If something goes wrong – say a security breach of personal data – users can't easily take TikTok to court. It's the standard Big Tech playbook: require private arbitration and prevent collective legal action, thereby reducing the company's litigation risk from its millions of consumers.

amazon

Amazon makes no representations or warranties of any kind, express or implied, as to the operation of the Amazon services or the information, content, materials, products… provided via the services. You expressly agree that your use of Amazon services is at your sole risk.”

AMAZON’S BLANKET DISCLAIMER OF WARRANTIES

This means that Amazon is saying its site and all its services come with no guarantees. If information on a product page is wrong or the site goes down during your purchase, Amazon is not on the hook via these terms. They even disclaim implied warranties like merchantability or fitness for a purpose.

While warranty disclaimers are common online, it’s striking given Amazon’s size – the company wants all the benefits of user trust and engagement without the typical consumer protections that products or services normally carry.

Google

In all cases, Google and its suppliers and distributors will not be liable for any loss or damage that is not reasonably foreseeable.”

GOOGLE’S NO LIABILITY FOR UNFORESEEABLE DAMAGES

This clause can shield Google from a wide array of consequential damages. For example, if a small business loses revenue because Gmail went down (an arguably unforeseeable chain reaction), Google’s terms say they owe nothing. The phrase “not reasonably foreseeable” is subjective and gives Google wiggle room to deny responsibility for anything beyond direct, obvious harms, which in a complex digital economy could leave users absorbing their own losses.

facebook

You agree to indemnify and hold the Company harmless from any loss, liability, claim, demand, damages, costs and expenses, including reasonable attorneys' fees, arising out of or in connection with… your use of the Service, your conduct in connection with the Service, or any violation of any law or the rights of any third party.”

FACEBOOK’S BROAD INDEMNITY CLAUSE

In non-lawyer terms, if your use of Facebook causes Facebook to get sued or incur costs (even due to something users might consider Facebook’s fault), you have to pay Facebook back for it. That’s what indemnification means. It puts the financial risk on the user for a huge range of issues. For instance, if you posted something and someone else claims it’s libel or IP infringement and drags Facebook into the lawsuit, Facebook’s terms say you must cover Facebook’s expenses. It’s a heavy burden that most users are unaware of when posting a meme or a comment.

Amazon does not warrant that the Amazon services, information, content, materials, products (including software) or other services included on or otherwise made available to you… are free of viruses or other harmful components."

AMAZON SAYS "AS IS" – INCLUDING VIRUSES

This is Amazon essentially saying: "Use our website or downloads at your own risk; if you get a virus from something on Amazon, that's not our responsibility." It's a CYA ("cover your ass") statement common in software licenses, but seeing it in consumer-facing terms is a reminder that even on trusted sites, companies refuse liability if their platform inadvertently distributes malware. It underscores a lack of recourse if a bad actor were to, say, offer a virus-infected file through an Amazon service.

Microsoft's Services Agreement and Privacy Statement allow using data from services like Outlook.com or Skype to target ads (though Microsoft says it doesn't use email content for ads, it does use other usage data). The ambiguity comes in clauses where users agree that Microsoft may "use data from your interactions" to personalize your experience.

MICROSOFT 365 DATA USE FOR ADVERTISING:

The average person using a Microsoft product (Office online, or a free Outlook email) might not expect that their activity is being mined for advertising or product improvement. Microsoft's terms are often broad about data use, lumping together functional telemetry with advertising. This blurriness means users effectively consent to a level of behavioral tracking without realizing it. While not as notorious as Google or Facebook on this front, Microsoft still leverages user data commercially under cover of its sweeping terms.

Snapchat's Terms grant them "a *worldwide, royalty-free, transferable, sublicensable, and irrevocable license to host, store, use, display, reproduce, modify, adapt, edit, publish and distribute" content you post, even for Snaps that disappear.

SNAPCHAT'S SELF-DESTRUCT ISN'T ABSOLUTE (LICENSE TO SNAPS)

Snapchat built its brand on ephemerality – photos that vanish – yet its terms allow Snapchat to save and use your snaps (for example, stories or any content submitted to public areas) as it sees fit. Users often don't realize that Snapchat's servers can keep content and the company can utilize those "disappearing" messages in accordance with its terms (say, for a safety investigation or to comply with a legal request). The disconnect between the app's image and its actual policy is a transparency issue.

In TikTok's terms, users agree that TikTok may "modify, adapt, or create derivative works from your content". This means if you make a popular dance video, TikTok can remix or edit that video (or let others do so) for promos or features without needing your approval.

TIKTOK'S RIGHT TO MODIFY YOUR CONTENT (FOR ADS)

TikTok's culture thrives on remixes and duets, and the terms basically ensure users can't object to how their videos are altered or repurposed. While it fuels creativity on the platform, it also means losing control. For instance, your video could be cut and used in a context you didn't intend, but TikTok immunizes itself from any claim you might have about that misuse by having you pre-authorize modifications.

LinkedIn's terms include consent to use your name, profile picture, and information in sponsored content or ads (for example, telling your connections that you liked a company page).

LINKEDIN'S RIGHT TO USE YOUR PROFESSIONAL INFO IN ADS

Many users have seen their face and name pop up in their connections' feeds endorsing something passively. LinkedIn leverages the fact that what you do on the platform (follow a company, recommend a skill) can be broadcast as promotional material. The terms effectively say you allow LinkedIn to take your actions and identity and weave them into native ads to others. It's a reminder that even seemingly benign professional interactions can be harnessed for marketing.

Spotify's Terms note that they can change the subscription fee and features and "will notify you in advance… and if you continue to use the service, you accept the new terms." It also disclaims liability for interruptions or errors in the service.

SPOTIFY'S CHANGE-YOUR-PLAN CLAUSE

In practice, it means Spotify can raise prices or alter what you get (say, limit device switching or sound quality) with a notice, and if you don't cancel, you're deemed OK with it. Many subscription services have this, giving them flexibility to adjust offerings. But for users, it means the plan you signed up for isn't guaranteed – your $9.99 for ad-free music might become $10.99 or develop new limits, and your only choice is to accept or quit (there's no negotiation).

Google Play’s terms say that digital purchases are generally “non-refundable” and any exceptions are at Google’s discretion; also, “Google is not responsible for third-party content” on the store.

GOOGLE PLAY STORE’S REFUND POLICY CAVEAT

If you buy a dud app or an ebook by accident, Google Play’s fine print indicates you might be out of luck on a refund (even though in practice they often grant refunds within a short window). The bigger picture is the store disclaims responsibility for apps – so if an app scams you or malfunctions and causes loss, Google distances itself via terms. Users often assume the platform will help if something goes wrong, but contractually Google places the risk on you (and maybe the app developer, who is often hard to reach).

We Can Remove Apps You've Bought: Apple's media and App Store terms include that "Content may be removed from the Services at any time… Apple shall not be liable for losses if previously purchased content becomes unavailable for re-download."

APPLE'S APP STORE RULE

If you paid for a movie, song, or app, you might assume it's yours forever. But Apple reminds you that digital purchases are more like rentals tied to their ecosystem. If licensing deals change or an app is yanked, you could lose access and Apple isn't going to compensate you. This clause is a stark example of how owning something on paper (or rather, on-screen) is not the same as a physical purchase; your access is subject to the continuing agreement between Apple and the content provider.

X's Terms summary notes "We may… terminate your account for other reasons, such as prolonged inactivity."

TWITTER (X)'S AUTHORITY TO BAN FOR INACTIVITY

If you take a Twitter hiatus for too long, the company says it can pull your handle and account. This shows how your presence on a platform isn't fully in your control; even doing nothing (literally) can be grounds for losing your account identity. People have felt the sting of this if a beloved account is deactivated due to inactivity. It's a minor clause but underscores that your account is essentially on loan, not owned by you, even if you were the one to build its following.

prime video

Deep in Amazon's conditions for Prime Video, there's language that the content is provided as-is, and "Amazon is not liable for cinematic quality or for the viewer's experience".

AMAZON PRIME VIDEO'S NO LAWSUITS OVER QUALITY

This means if a film streams in poor resolution or an episode is mislabeled, you can't claim damages or breach – at most, you get a refund for that rental or similar. It's Amazon preemptively cutting off any claim that the service didn't deliver what was promised, beyond maybe a customer-service courtesy credit. Essentially, they guarantee nothing about the quality of streaming (outside what consumer law compels). As streaming replaces owned media, this shows how little recourse consumers have if the quality is subpar or features are removed.

In 2021, YouTube added that “YouTube has the right to monetize all content on the platform and ads may appear on videos from channels not in the YouTube Partner Program.” In other words, even if you’re a small creator who isn’t earning ad revenue, YouTube can run ads on your videos and keep the money.

YOUTUBE’S RIGHT TO MONETIZE ANYTHING

This rubbed a lot of users the wrong way. It means YouTube can plaster ads on a video you upload of your kid’s birthday or your free tutorial and you get $0 from it. Previously, no-ads was a quasi-perk for non-monetized channels. The clause exemplifies an imbalance: YouTube/Google unilaterally decided to profit from all user content, changing a norm on the platform via a TOS update. It’s a reminder that what you consider your content, they might see as their ad inventory.

WhatsApp's terms allow account suspension not just for in-app violations but if "we believe you are infringing the rights of others or engaging in unlawful, obscene, harassing, or objectionable activities" – which could include outside of WhatsApp.

WHATSAPP CAN SUSPEND FOR "HARMFUL" BEHAVIOR OFF-APP

This broad morality clause means your account can be banned based on things not even said on WhatsApp. It's an example of an ambiguous standard ("objectionable" to whom?) that grants the company wide latitude. In practice, WhatsApp might use this to ban users associated with hate groups or misinformation elsewhere. But for users, it's a vague threat: your private messaging access is conditioned on your general good behavior as judged by a private company.

facebook

Facebook's policies admit they collect data about people who don't even have an account, via plugins, cookies, etc. (e.g., "Facebook stores cookies on browsers even if you do not have a Facebook account").

FACEBOOK STORES DATA ON NON-USERS

This is not in the user TOS per se, but it's in the privacy policy and revealed in investigations. It means even if you never agreed to Facebook's terms, Facebook might have a "shadow profile" on you. For citizens, that's a rights issue: being tracked without even signing up. It shows how Big Tech's reach extends beyond contractual users – they effectively impose surveillance on the broader public, which terms and conditions don't cover (since there's no agreement). It raises questions of fairness and transparency far outside the normal user-company relationship.

You agree not to reverse engineer, decompile, disassemble or attempt to derive source code from our software.” This typical clause (present in many services) is in LinkedIn’s terms to prevent users from tinkering with or analyzing their platform’s code or algorithms.

LINKEDIN’S NO REVERSE ENGINEERING CLAUSE

On its face, this protects intellectual property. But it can also stifle accountability and transparency. For instance, if an independent researcher wants to study LinkedIn’s algorithm for potential bias (say in job recommendation visibility), this clause could be used against them. It’s a somewhat controversial aspect because it pits user rights and academic freedom against corporate secrecy. In broader context, Facebook famously used similar terms to send cease-and-desist letters to researchers investigating political ads. So, these anti-reverse-engineering terms can have a chilling effect on understanding what these platforms are really doing under the hood.

Similar to PayPal, Cash App's terms note that violating their rules can lead to account termination "and your funds could be held for an indefinite period".

CASH APP'S ACCOUNT TERMINATION AND FUNDS FORFEIT

Mobile payment apps like Cash App (Square) or Venmo follow the template: break the rules (even unknowingly) and you might lose access to your money. It's often framed as anti-fraud or compliance with law, but for users it means you're at the mercy of an opaque review if algorithms flag something. Innocent people have had money frozen due to false positives. The controversial part is the indefinite nature and lack of due process spelled out – the company writes itself a carte blanche to hold or seize funds with minimal explanation.

Microsoft's communication services (Skype, Teams) include that "Microsoft may monitor your communications to the extent permitted by law" for certain purposes like enforcement or improving the service.

SKYPE/TEAMS MONITORING CONSENT

Real-time communication apps usually promise privacy, but the terms often allow some level of monitoring or scanning (often for abuse or security). Microsoft's caveat is a bit unsettling: it reminds users that private calls or chats are subject to being observed or recorded by the company if deemed necessary. While they likely rarely use this except in obvious abuse cases, it's a crack in confidentiality that users might not expect from their video calls or chats.

Slack's policies (for certain paid workspaces) let an employer export all workspace data, including what users think are private 1:1 or small-group messages, if they go through a compliance export process.

SLACK'S EXPORT OF PRIVATE CHATS

In workplace communication, the company's terms essentially say your boss can obtain everything you say on Slack. Slack's own terms with users defer to the workspace admin's rights. This has been controversial as employees often treat Slack like a casual texting zone, not realizing their DMs can be later read by HR or legal. It's a clash between expectation and reality set by fine print (and admin settings). While not an "abuse" by Slack per se, it's a user rights issue that many learn about the hard way.

Reddit's User Agreement claims a "royalty-free, sublicensable, perpetual license to use and display your content" — with some limits.

REDDIT'S LICENSE TO USER POSTS

Reddit communities run on user submissions. The terms ensure Reddit can, for example, show your posts in marketing materials or create derivative works (perhaps a published anthology of best Reddit comments?) without needing your permission. Users retain ownership, but Reddit's license is broad enough that you effectively share ownership with Reddit for anything you post. Given many people post personal stories or creative content on Reddit, this license can be seen as overreach – but it's how Reddit legally protects its ability to operate (and make money off) the content that users entirely provide.

The chat platform Discord requires disputes to go to arbitration and forbids class actions (with an opt-out available if done in time).

DISCORD'S ARBITRATION AND NO CLASS SUIT CLAUSE

Discord, popular among gamers and communities, quietly includes the same kind of legal restrictions as the big players. Young users especially might not realize they've signed away the right to sue Discord in court or join a class-action. If, for instance, a privacy scandal happened with Discord, each user would have to arbitrate individually (unless they opted out of that clause within 30 days of sign-up by snail mail). It's a stark example of industry-standard terms appearing even in services perceived as more community-driven or informal.

Tinder's terms ban under-18s (standard) and also note they "may use information about you from public sources for safety and verification".

TINDER'S AGE RESTRICTION AND DATA USE

The latter means the dating app might scrape your social media or do web searches to vet users. While many would welcome safer dating, it raises eyebrows that by agreeing to terms, you consent to Tinder doing potentially deep digs on your online presence. Where they draw that line isn't clear, and it puts a lot of trust in Tinder to handle whatever they find appropriately. Additionally, Tinder's terms also limit liability extensively (imagine if a date goes wrong – Tinder positions itself as not legally accountable as it just introduces people). All told, dating app terms often highlight a tension between user safety, privacy, and company liability avoidance.

WhatsApp imposed a technical limit (you can only forward a message to 5 chats at once to curb spam/misinformation). Their terms enforce that users agree not to bulk forward in ways not provided by the app.

WHATSAPP'S FORWARDED MESSAGES LIMITATION

This shows how terms can reach into specific user behaviors. It's not just broad legal language; it can dictate how you actually use the features. If someone found a workaround to forward a message to 100 groups, they'd be violating the terms. This is slightly controversial as a free speech issue – some users chafe at being told how they can share information. But it also speaks to a platform taking responsibility (via terms and design) for curbing viral rumors. It highlights that terms of service can be a tool for shaping user conduct on a granular level.

Virtually every platform has a clause akin to: “We reserve the right to remove or take down any content you post, for any or no reason.” For example, YouTube: “YouTube may terminate your access, or remove any content you have contributed, in its sole discretion, without notice.”

GENERIC “WE CAN REMOVE CONTENT” CLAUSE

This catch-all content removal right is controversial when platforms moderate in ways users feel are unfair (too harsh or not harsh enough). From a user rights perspective, it means you have no guaranteed freedom of expression on these private services – your posts exist only as long as the company tolerates them. While companies invoke this to remove hate speech or illegal content, it also means they could remove content for murkier reasons (critical posts, competitive links, etc.) and users have little recourse because they technically agreed to it. It’s the foundational clause enabling all platform content moderation, for better or worse.

(We've now seen how companies claim far-reaching powers in their terms – from watching everything you do, to using your data however they like, to denying you the chance to fight them in court. But there's more.)

IV

MORE FIFTY TONES OF CORPORATE SHADE

(The core pattern across these 50 sneaky terms is the profiteering over **power asymmetry**

—not just in a legal or financial sense, but in infrastructure, behavioral design, and emotional dependence.

The shift we see here is from companies offering services to companies designing ecosystems where the user is no longer just a customer—but a participant, a data source, and a liability.

1.

AT OUR DISCRETION

Almost every clause grants the platform total authority to:

Suspend accounts arbitrarily (eBay, Microsoft Teams, Proton)

Remove content or features (Zoom, Adobe, Hulu, Medium)

Downgrade or restrict access (Dropbox, Disney+, Flickr)

This is not just about control—it's about unilateral control, insulated from recourse.

2.

OWNERSHIP AND SURVEILLANCE

Across platforms, you "retain ownership" of your content or identity, but the company gets a broad, royalty-free, perpetual license (Epic, OkCupid, Pinterest, Ring).

Paired with:

Deep tracking (Amazon, YouTube Kids, Mozilla, Waze), licensing of location or behavioral patterns, use of private conversations for “improvement” or ads.

3.

ARBITRATION, ISOLATION, NEGATION

Dozens of these companies enforce:

- **Mandatory arbitration**
- **No class action rights**

User liability in cases of platform failure (Coinbase, Mastercard)

This cuts off collective redress—turning systemic harm into isolated frustration.

4.

HOSTAGEWARE!

You pay, and still:

Can't get refunds (Slack, Nintendo, Adobe)

Can be denied access (Sony, Valve, Dropbox)

Are at risk of account deletion or shadow restrictions at any moment (Tumblr, WordPress)

These companies know their platforms are part of your digital identity or livelihood, and use that dependency as leverage.

5.

DESIGN FOR AMBIGUITY

“We may…”

“At our discretion…”

“As permitted by law…”

These phrases legitimize absolute control, with no clear reasoning, while keeping them under a tone of neutrality.

“If a dispute arises between you and eBay, our goal is to provide you with a neutral and cost-effective means of resolving the dispute quickly… You and eBay agree to resolve any claim or dispute at law… in accordance with this arbitration agreement.”

EBAY’S MANDATORY BINDING ARBITRATION (U.S. USERS)

Users can’t bring eBay to open court for most disagreements; they’re forced into private arbitration. This is standard in the industry but still curtails class-action options.

“We may limit, suspend, or end your user account… at our sole discretion.”

EBAY’S SELLER SUSPENSION FOR UNSPECIFIED REASONS

If eBay suspects suspicious activity or sees potential risk, it can freeze your seller account. Sellers often complain they’re cut off from their own inventory listings without a clear reason or recourses.

“Zoom may modify, update, or discontinue the Services at any time without liability to you.”

ZOOM’S “SERVICE MODIFICATIONS” CLAUSE

Zoom can remove features (like unlimited group calls or specific collaboration tools) unilaterally. Users relying on certain features might find them suddenly gone, with no compensation.

“You acknowledge that you may be recorded… Zoom is not responsible for the actions of other participants in the meeting.”

ZOOM’S RECORDINGS AND CONFIDENTIALITY DISCLAIMER

While meeting hosts must get consent before recording, Zoom itself disclaims any responsibility if participants record or share the footage elsewhere. This leaves end users vulnerable if sensitive content is circulated.

“You grant Epic a worldwide, royalty-free, sublicensable license to use, modify, reproduce… your UGC.”

EPIC GAMES (FORTNITE) ON USER-GENERATED CONTENT

Gamers designing custom Fortnite maps or content effectively license their creations to Epic in perpetuity. Although common in creative platforms, it’s a broad right many don’t notice.

“We may install and use software to detect cheating… which may scan your device to detect unauthorized third-party programs.”

EPIC GAMES’ ANTI-CHEAT SOFTWARE MONITORING

This monitoring can raise privacy concerns, as it typically operates at a deep system level and can inspect files or processes to spot cheats.

“Fees paid are non-refundable, including if you downgrade your plan before the end of your subscription term.”

SLACK’S “NO REFUND” POLICY

If you decide Slack’s advanced plan isn’t what you needed, you’re stuck paying until the term ends. It’s a standard subscription model practice but can catch smaller teams off-guard.

“We may access your Workspace Data for the purpose of providing and maintaining the Services…”

SLACK’S RIGHT TO ACCESS WORKSPACE DATA

Slack staff can, in principle, read stored chats or files for operational reasons. Though presumably minimal, the clause is open-ended, and users often assume chats are strictly private.

“You agree to let Adobe install updates automatically… You may not be able to reject or delay updates.”

ADOBE CREATIVE CLOUD FORCED UPDATES

Adobe can push updates to your devices that could change functionality or system requirements, with limited user control. This ensures security patches, but also can break workflows or older hardware compatibility.

“We may discontinue older versions of the Services and access to those versions at any time.”

ADOBE’S TERMINATION OF ACCESS TO OLDER VERSIONS

Designers reliant on a stable older version of Photoshop, for instance, might see it retired, leaving them forced to upgrade or lose access.

“We may share information about your listening habits, such as songs you stream, with certain partners to help them understand user trends.”

SPOTIFY SHARING “LISTENING DATA” WITH PARTNERS

Some listeners are uncomfortable that data on every track played could be sent to third parties (labels, analytics firms, advertisers) for various profiling purposes.

“Unless you cancel your subscription prior to the end of the applicable subscription period, it will automatically renew…”

SPOTIFY’S AUTO-RENEW SUBSCRIPTION IN ALL REGIONS

Many forget to cancel free trials or monthly plans, resulting in repeated billing. This is typical but still a frequent source of user frustration and accidental charges.

“We may hold or delay payout of funds to you if we believe there is a risk of fraud or other forms of misconduct.”

SHOPIFY’S CONTROL OF PAYMENT PAYOUTS

Small online merchants can have earnings held back—sometimes for weeks— if Shopify’s system flags potential risk. This can disrupt cash flow with minimal explanation from the platform.

“We are not responsible for third-party apps you install… any issue arising out of their use must be resolved with the third-party developer.”

SHOPIFY’S “NO LIABILITY FOR THIRD-PARTY APPS”

If a plugin goes rogue or compromises store data, Shopify washes its hands of responsibility. Store owners might find it hard to pinpoint or rectify damage when a plugin fails.

“By using Mastercard, you consent to our collection and analysis of purchase data to the extent permitted by law.”

MASTERCARD’S PROPRIETARY DATA COLLECTION

Every time you swipe or tap, Mastercard logs the transaction details. While anonymized for analytics, the broad language allows significant data mining of your spending habits.

“Disputes are subject to arbitration… you waive your right to a class action, to the fullest extent permitted by law.”

MASTERCARD PROHIBITION ON CLASS ACTIONS

Credit card users rarely read this in the agreement from the issuing bank or card network. It’s another block to banding together for consumer rights claims, placing disputes into private arbitration.

“You may not reverse engineer, decompile, or attempt to discover the source code of the Apple Software.”

APPLE IOS DEVELOPER AGREEMENT: BAN ON REVERSE ENGINEERING

This is typical for protecting proprietary software, but it restricts security researchers who might want to find vulnerabilities or study how the OS handles data behind the scenes.

“Apps that do not comply with these guidelines may be removed at any time, and all fees paid are non-refundable.”

APPLE’S STRICT APP STORE RULE ENFORCEMENT

Developers risk losing their listing (and investment) if Apple enforces a policy in ways that devs might perceive as arbitrary or lacking transparency. They also have no recourse for refunds on developer fees.

“We may continue collecting location data… even if you are not actively using the Maps service, as permitted in your account settings.”

GOOGLE MAPS LOCATION COLLECTION EVEN WHEN IDLE

Users who forget to revoke location access can have passive location tracking. Google’s default opt-in sets up continuous geolocation logs unless you dig into settings to opt out.

“Waze collects certain traffic data and location data from your device to improve the Service for all users.”

WAZE (GOOGLE) CROWDSOURCING OF LIVE DATA

Though beneficial for real-time traffic routing, it’s another instance of near-constant data gathering. Many users embrace it, but it does raise the question of how long location logs are stored.

“We reserve the right to deactivate your account… if we have reason to believe it may cause harm to others or to Microsoft.”

MICROSOFT TEAMS “AT OUR DISCRETION” DEACTIVATION

This broad discretionary language means an entire team’s communication hub can vanish overnight if flagged. Though presumably rare, it’s a significant risk for enterprise or personal users who rely on Teams daily.

“We may use consumer reports to determine your eligibility for installment payments.”

PAYPAL DE FACTO “CREDIT CHECK” FOR PAY IN 4

PayPal effectively does a soft credit check for “Buy Now, Pay Later” or “Pay in 4.” While legal, some consumers might not realize they’re consenting to a credit inquiry that can appear on credit bureau data.

“We reserve the right to determine how and where listings appear and to remove or delist restaurants in our sole discretion.”

UBER EATS RESTAURANT LISTING AUTONOMY

Restaurants can be pushed down in search results or removed entirely, often without explanation. For small businesses, that can drastically impact visibility and income.

“Lyft is not responsible for any items left in a vehicle by riders.”

LYFT’S ZERO LIABILITY FOR LOST ITEMS

Even if you can track your driver, Lyft’s terms disclaim liability for anything left behind. While the driver or support might help, the official stance is that you’re on your own if valuables vanish.

“In times of congestion, your data usage may be prioritized behind other traffic, impacting speeds.”

T-MOBILE DATA PRIORITIZATION NOTICE

T-Mobile acknowledges they can slow certain users compared to others during peak traffic, a less severe form of throttling but still a network management practice some find controversial.

“If your account is terminated, your wallet balance and any rights to content are immediately forfeited.”

SONY PLAYSTATION NETWORK BALANCE FORFEITURE

If Sony bans you for violation (even a contested one), you lose all purchased games, add-ons, or store credit. It underscores how digital goods can vanish if the platform cuts you off.

“All purchases made on Nintendo eShop are final, and no returns or refunds will be offered, except where required by law.”

NINTENDO ESHOP REFUND POLICY

If you accidentally buy the wrong game or regret a purchase, you likely won’t be able to return it. The “required by law” exception is typically minimal in many jurisdictions.

“Valve may stop distributing any or all Content at any time… or cease making certain features of Steam available.”

STEAM’S (VALVE) CONTENT AVAILABILITY CLAUSE

If a developer pulls a title from Steam, or if Valve decides to delist it, you might lose the ability to download or update that game. Steam rarely removes purchased games, but the right is in the TOS.

“By creating an account, you grant us a worldwide, royalty-free license to host, store, use, copy, display, reproduce, adapt, edit, publish, modify and distribute the information you post… We may also collect and use any information that you provide through chats, surveys, or messages, to improve our products, features, and advertisements, as well as to share with third-party partners.”

OKCUPID’S “EXHAUSTIVE USE OF PERSONAL DATA” CLAUSE

OkCupid (under Match Group) already gathers detailed information about a user’s relationships, preferences, and personality through its in-depth questionnaires. This clause expands their right to use that data in nearly any way they see fit, including sharing it with third parties for targeted ads or product development. Because many questions delve into sensitive topics (e.g., political views,

religion, sexual preferences), the broad license to store, analyze, and share that data raises concerns about user privacy and profiling.

> “You expressly understand and agree that we will not be liable for any losses, damages, or claims arising from: (a) user error, such as forgotten passwords or mistyped wallet addresses; (b) server failure or data loss; (c) corrupted wallet files; (d) unauthorized access to applications; (e) any unauthorized third-party activities… Any dispute related to these Terms shall be resolved by binding arbitration and not in a court of general jurisdiction.”

COINBASE’S “NO LIABILITY FOR CRYPTO VOLATILITY” AND FORCED ARBITRATION

The cryptocurrency world is prone to extreme price fluctuations, security breaches, and regulatory uncertainty. Coinbase’s terms disclaim responsibility for almost every risk imaginable—even some that might stem from platform vulnerabilities. Additionally, users must sign away the right to sue in a public court or join a class action, forcing them into private arbitration if Coinbase’s security measures fail or if they face unaddressed losses. This structure heavily shields the company from large-scale legal accountability while leaving individual users with limited recourse when problems arise.

> “Some data may be collected to support features like content recommendations, to the extent permitted by law.”

YOUTUBE KIDS “DATA FROM CHILDREN” NOTICE

Though YouTube Kids follows child-privacy rules, it still tracks user interactions to recommend content. Critics argue that any data-gathering from children is worth scrutiny, even if it’s limited.

“If payment cannot be processed, we may downgrade your subscription features or terminate the account.”

DISNEY+ AUTOMATIC DOWNGRADE ON FAILED PAYMENT Users who simply miss a payment could find themselves with a downgraded plan or locked out of their library. Disney’s approach to lapsed billing is standard but can feel abrupt.

“Content is subject to change at any time. Some programming may expire or be removed from the Service without notice.”

HULU’S RIGHT TO CHANGE AVAILABLE CONTENT Your favorite show might vanish overnight due to a licensing change. This is how streaming deals work, but the lack of notice can be jarring when it disrupts your nightly binge.

“Alexa processes and retains voice inputs to improve the service and develop new features…”

AMAZON DEVICES COLLECTING VOICE SAMPLES
Even if you delete a specific recording, Amazon’s broader TOS indicates the system still learns from your input. This is valuable to Amazon’s AI but can unnerve those who want ephemeral voice data.

“You retain ownership of Content… but grant Ring a license to use, copy, distribute, and store your Content… to provide and improve the Service.”

RING (AMAZON) VIDEO OWNERSHIP AND ACCESS
Security footage from your doorbell is technically yours, but you still give Ring wide latitude for usage. And if law enforcement requests it, Ring has a track record of cooperating with minimal user involvement.

“Oracle may audit your use of the Services (including software) to verify compliance with the terms.”

ORACLE CLOUD “OPEN TO AUDIT” CLAUSE

Large enterprise customers sign up for this, but the concept of letting Oracle’s auditors examine your systems is nerve-wracking. Audits can be invasive, though typically scheduled.

“IBM’s liability for any damages arising out of this Agreement shall not exceed the amount paid by you for the relevant Service during the 12 months preceding the event.”

IBM CLOUD LIMITATION OF LIABILITY

Even if a major glitch in IBM Cloud costs you huge sums, you can only recover up to what you paid IBM. Typical of enterprise deals, but it shows how big providers insulate themselves from large damage claims.

“We may use aggregate or de-identified data from your use to improve or develop new Salesforce services.”

SALESFORCE DATA ANALYTICS USE

While less personal, the line between “de-identified” and real personal data can be blurry if data can be re-linked. The language is standard, yet some enterprise clients want clearer guardrails.

“If you don’t pay on time, we may suspend your account (or reduce functionality) after 30 days.”

DROPBOX’S 0-DAY ACCOUNT SUSPENSION FOR NON-PAYMENT

This is typical, but for individuals or businesses that rely on Dropbox for mission-critical files, losing access can be devastating. The TOS basically says your data is hostage until you clear the bill.

“You may not use Proton services in any manner that is considered (in our sole judgment) to be unlawful, offensive, or harmful.”

PROTONMAIL ACCEPTABLE USE: BROAD INTERPRETATION

ProtonMail is known for privacy, but it can still shut you down if it deems your activity “harmful” — a subjective standard. They rarely exercise it without cause, but the language is broad.

“You use Signal at your own risk, and we make no warranties, express or implied, about reliability or accessibility.”

SIGNAL’S NO WARRANTY CLAUSE

Despite being lauded for secure messaging, Signal won’t guarantee 100% uptime or data protection. If the service fails or messages disappear, you have limited recourse.

“By default, Firefox sends data about your usage, such as performance and feature usage data, to Mozilla.”

MOZILLA FIREFOX TELEMETRY COLLECTION

Though Mozilla is a nonprofit, it still collects “telemetry” unless you opt out. Telemetry is standard, but some privacy-focused users dislike default data gathering even from a pro-privacy brand.

“If you upload content as publicly viewable, you grant Vimeo the right to embed advertising or promotional content around or within your video.”

VIMEO’S RIGHT TO MONETIZE PUBLIC VIDEOS

Vimeo historically branded itself as ad-free, but these terms note they can place ads on or near public videos at their discretion. Could be contradictory to user expectations.

“We may promote or remove your stories at our sole discretion based on editorial or algorithmic determinations.”

MEDIUM’S CURATION & DISTRIBUTION ALGORITHMS

Your post might vanish from recommendations or be heavily featured, with zero transparency about how Medium’s editorial or AI picks winners. Writers effectively gamble on an opaque system.

“Tumblr may remove content that it deems pornographic or otherwise in violation of community guidelines…”

TUMBLR’S ADULT CONTENT PURGES

After policy changes, Tumblr purged adult content. The TOS allowed wide latitude for removal, which blindsided many users who had posted such content for years. The shift left some feeling they’d lost an important community space.

“Yahoo may analyze emails for ad targeting and spam/malware detection.”

YAHOO MAIL SCANNING FOR ADS

Like Gmail, Yahoo’s scanning goes beyond security—it’s also for personalized advertising. This broad scanning is typical but still a privacy compromise.

“We are not responsible for any third-party content, bots, or interactions you have through the Telegram platform.”

TELEGRAM’S “NO LIABILITY” FOR THIRD-PARTY BOTS

Bots can harvest data or scam users, but Telegram shifts liability to the bot creators. Users might believe Telegram endorses or vets these bots; the TOS says otherwise.

“By posting content, you grant Pinterest and its users a non-exclusive, royalty-free license to save, share, and show that content.”

PINTEREST’S USE OF YOUR PINS

It’s central to Pinterest’s functionality, but it means once you pin something, you can’t complain if it circulates widely. Many users think it’s just their board, but the content can propagate everywhere.

“If you exceed your free storage limit and do not upgrade, we reserve the right to remove content or terminate your account.”

FLICKR’S ACCOUNT DELETION OVER FREE STORAGE LIMIT

Flickr drastically reduced free storage in 2019. Users with huge historical libraries risked losing photos if they didn’t pay or move them elsewhere, a jarring shift from earlier “generous” free tiers.

“Automattic (WordPress.com) reserves the right to remove any content that it determines is unlawful, offensive, or otherwise objectionable.”

WORDPRESS.COM CONTENT TAKEDOWN AT “SOLE DISCRETION”

A standard moderation clause, but “otherwise objectionable” is broad. For those relying on WordPress.com for blogging, that leaves final editorial authority in corporate hands.

(Many of these policies revolve around forced arbitration or liability limits—themes common across industries.

Data and content usage rights show up repeatedly, reflecting the tension between user privacy and corporate data exploitation.

Service flexibility—the right to remove content, change features, or terminate accounts without recourse—is everywhere.

Even well-regarded brands known for privacy or user-centric policies (e.g., Mozilla, Signal, ProtonMail) still include standard disclaimers that curb user protections.

Across consumer tech, enterprise software, and payment platforms alike, the fundamental pattern is

that the company retains the final say over your data, your content, or your continued membership, often “at their sole discretion.”)

Byung-Chul Han wrote that in the digital era, we do not rebel—we accept. Transparency is weaponized, and data is extracted not by force, but by the emptied ritual of clicking “I agree.”

The last 50 examples in this book are not flaws, they are features of an optimized system that diluted checks and balances, while under a compelling narrative that bestows the responsibility of such terms onto the user, even de-coupling the citizen, who has civic rights and obligations, from the user, who operates within the platform logic.

V

TOP OFFENDERS AND DISHONORABLE MENTIONS

- **Control across device, app, cloud, voice, and data layers.**
- **Their terms span hardware surveillance (Alexa, Ring) to content control (YouTube, Maps) to data inheritance rights.**
- **They blur consumer use and backend exploitation.**

1

Meta amazon Google

ECOSYSTEM OVERLORDS

- **Exploit creators through forced updates, data mining, perpetual licenses.**

- **Anti-cheat surveillance, content royalties, and removal of past versions keep users on a treadmill.**

2

CREATIVITY LOCK-INS

- **Normalize throttling, forced arbitration, and user-funded risk coverage.**

- **They combine behavioral profiling and corporate shielding in sectors where user choice is limited.**

3

COURTROOM PROFESSIONALS

- **OkCupid & Match Group: Extremely sensitive user data, shared broadly.**
- **Coinbase: Zero liability stance, despite handling volatile assets.**
- **Slack: Can read chats, gives no refunds, owns your workspace.**
- **Shopify: Can freeze your cash**

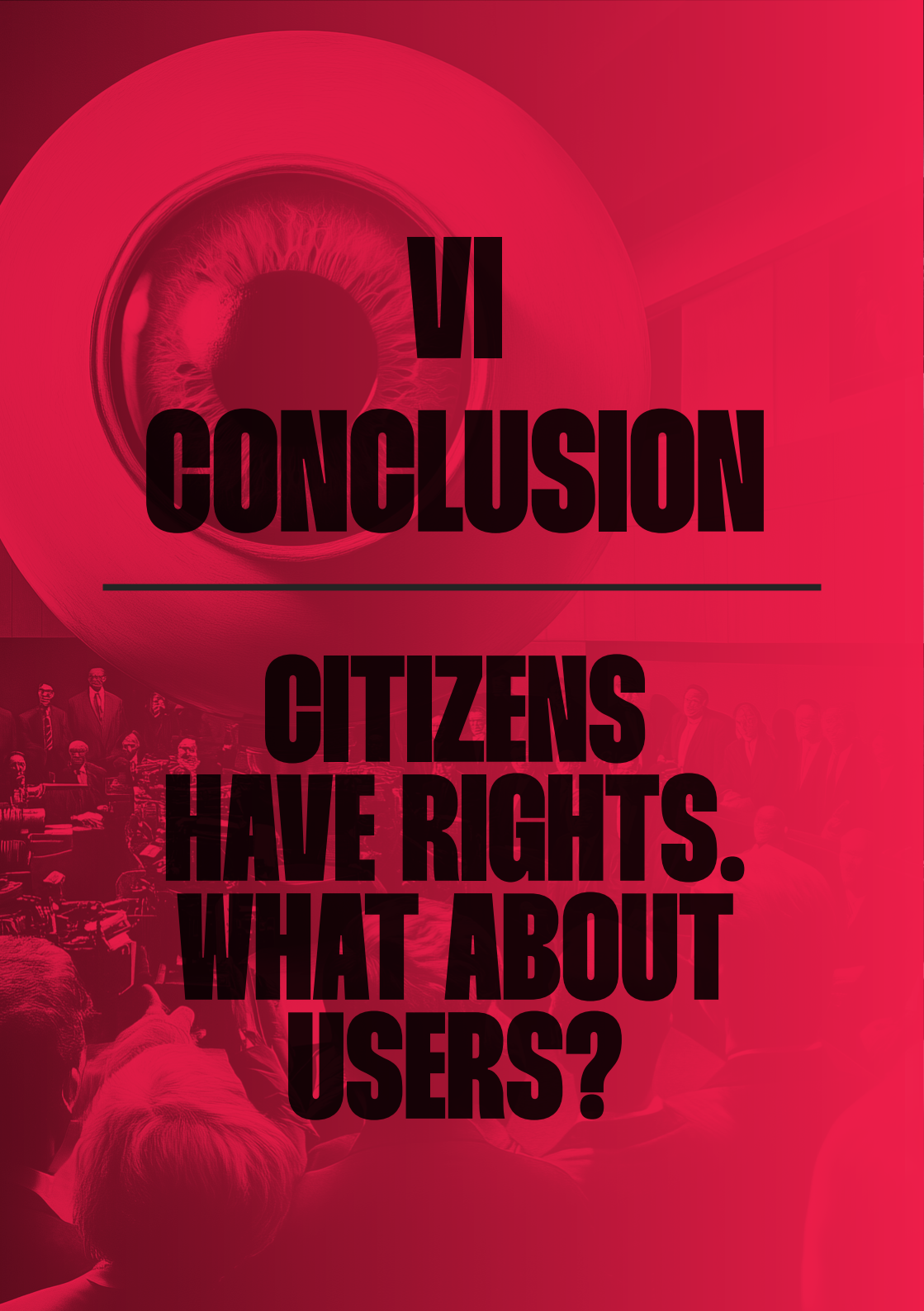
okcupid coinbase

shopify

DISHONORABLE MENTIONS

VI
CONCLUSION

CITIZENS HAVE RIGHTS. WHAT ABOUT USERS?



THE CONFUSION BETWEEN BEING A CITIZEN AND BEING A USER ERODES THE RIGHTS OF BOTH

At the heart of any democracy lies a set of shared rights—due process, representation, the ability to face one's accuser. But within the walled gardens of digital platforms, those rituals are rendered void. A striking number

of platforms now require users to give up their right to a public trial, opting instead for private arbitration, shielded from collective redress and regulatory scrutiny.

Consider:

You give up your legal rights. eBay, Coinbase, Mastercard, and Apple all include binding arbitration clauses that bar users from pursuing legal action in court or joining class-action lawsuits.

PayPal, Slack, and Adobe similarly include language that shifts legal disputes into private forums where platform policies—not civic values—rule.

These clauses are not fringe cases. They are, in fact, industry

standard—widely accepted conditions that govern the platforms we rely on daily. Binding arbitration. Unilateral suspension. Non-refundable access to content you thought you "owned."

At a glance, these might seem like the fine print of convenience. But at a deeper level, they mark a growing distance between the legal norms of citizenship and the contractual norms of platform life.

In theory, a citizen has the right to due process, to face their accuser, to appeal. In practice, the user—on eBay, Coinbase, Mastercard, PayPal, Adobe, Apple, and so many others—has agreed not to go to court, not to speak collectively through a class action, not even to contest in public. They

are bound to private, opaque arbitration, overseen not by civic institutions, but by the platform itself or third parties it designates.

This would be less troubling if these platforms were marginal. But they're not. They are the infrastructure of daily life—where we work, learn, shop, communicate, date, bank, and move. As such, they function increasingly as the de facto public square of the digital age.

And yet, within that square, a different logic rules.

THE TRIUMVIRATE OF EROSION

The erosion of digital rights isn't random—it is strategic. And it is driven by three interlocking forces:

OPAQUE. These terms are unreadable by design. Legal jargon, nested clauses, and opt-out options buried beneath UI layers create a fog of ambiguity. The less clear the system, the easier it is to normalize exploitative conditions.

OUTPACE. Legislators often trail

far behind technological realities. Platforms exploit this delay to entrench behaviors before watchdogs catch up. In many cases, regulators rely on the companies themselves to explain what's happening—further blurring lines of accountability.

PERFORMANCE. Financial power tilts the policy landscape. Companies influence how privacy laws are written, when enforcement occurs, and who gets access to the tools of justice. It is no coincidence that arbitration clauses persist even in sectors touching essential services like banking, telecom, and housing platforms.

This triumvirate creates a frictionless dystopia: not one of

overt surveillance or violent control, but of smooth, silent compliance.At a glance, these might seem like the fine print of convenience. But at a deeper level, they mark a growing distance between the legal norms of citizenship and the contractual norms of platform life.

In theory, a citizen has the right to due process, to face their accuser, to appeal. In practice, the user—on eBay, Coinbase, Mastercard, PayPal, Adobe, Apple, and so many others—has agreed not to go to court, not to speak collectively through a class action, not even to contest in public. They are bound to private, opaque arbitration, overseen not by civic institutions, but by the platform itself or third parties it designates.

This would be less troubling if these platforms were marginal. But they're not. They are the infrastructure of daily life—where we work, learn, shop, communicate, date, bank, and move. As such, they function increasingly as the de facto public square of the digital age.

And yet, within that square, a different logic rules.

THEORETICAL LENS: CHUL HAN'S TRANSPARENCY TRAP

Philosopher Byung-Chul Han has written extensively about the shift from disciplinary societies (à la Foucault) to achievement societies—where individuals internalize responsibility, performance, and visibility as ideals. In The Transparency Society, Han warns that:

"The society of transparency is a

society of exposure and control, a society that dismantles privacy and inner life by forcing everything to become visible."

Ironically, the more transparent we become—as quantified selves, oversharing users, trackable citizens—the less visible power itself becomes. Control does not manifest through punishment, but through protocol through design.

And the click becomes a rite hollow in itself.

A TECHNOFEUDAL DRIFT?

Some have begun to describe this transformation not as a failure of capitalism, but as a mutation of it. In Technofeudalism: What Killed Capitalism, economist Yanis Varoufakis suggests that platforms have ceased to be participants in markets. Instead, they are the market—defining the rules, controlling the interactions, owning the infrastructure.

> "What we are witnessing is the return of feudal dynamics, only this time not on land, but in the cloud." — Yanis Varoufakis (2023)

In this light, the user is no longer a

consumer in a competitive marketplace, but a tenant of digital land, subject to rules they cannot negotiate. Access can be revoked. Property (a game library, a paid subscription, a stored file) can be forfeited. Due process is replaced by the platform's discretion. What's legal inside the system is what the system allows.

This is not feudalism in the traditional sense. But the analogy helps clarify what's missing: recourse, reciprocity, and rights. The civic scaffolding of liberal democracy—negotiation, appeal, deliberation—is simply not present in the interface.

.

THE RITUAL WITHOUT THE RIGHT

Perhaps the most striking feature of this new order is that its control does not feel authoritarian. There is no visible repression. No punishment. Only clicks. The checkbox becomes a ritual—a moment of quasi-civic performance, where agreement is enacted, but not empowered.

And so we find ourselves performing consent in an ecosystem where consent has no teeth.

We click to agree because we cannot proceed otherwise. We agree not to sue, not to join others, not to be heard. We give up civic protections in exchange for usability, for reach, for connection.

But perhaps what we're giving up isn't only legal. Perhaps we're surrendering something subtler: a relationship to power that includes us.

And if that is the case, then what begins as Terms & Conditions may end as a new kind of social contract—not one we debated or drafted, but one we accepted by default, five seconds at a time.

.

SOURCES

1. **Airbnb.** “Terms of Service.” ***Airbnb.*** Accessed 18 Mar. 2025.
2. **Amazon.** “Conditions of Use.” ***Amazon.*** Accessed 18 Mar. 2025.
3. **Amazon.** “Amazon Prime Video Terms of Use.” ***Amazon.*** Accessed 18 Mar. 2025.
4. **Amazon.** “Alexa Terms of Use.” ***Amazon.*** Accessed 18 Mar. 2025.
5. **Apple.** “iCloud Terms of Service.” ***Apple.*** Accessed 18 Mar. 2025.
6. **Apple.** “Media Services Terms and Conditions.” ***Apple.*** Accessed 18 Mar. 2025.
7. **Apple.** “Apple Developer Program License Agreement.” ***Apple.*** Accessed 18 Mar. 2025.

8. **Automattic (WordPress.com).** “Terms of Service.” ***WordPress.com.*** Accessed 18 Mar. 2025.

9. **Automattic (WordPress.com).** “Privacy Policy.” ***WordPress.com.*** Accessed 18 Mar. 2025.

10. **ByteDance (TikTok).** “TikTok Terms of Service.” ***TikTok.*** Accessed 18 Mar. 2025.

11. **ByteDance (TikTok).** “TikTok Privacy Policy.” ***TikTok.*** Accessed 18 Mar. 2025.

12. **ByteDance (TikTok).** “TikTok Community Guidelines.” ***TikTok.*** Accessed 18 Mar. 2025.

13. **Cash App (Block).** “Terms of Service.” ***Cash App.*** Accessed 18 Mar. 2025.

14. **Discord.** “Terms of Service.” ***Discord.*** Accessed 18 Mar. 2025.

15. **Discord.** “Privacy Policy.” ***Discord.*** Accessed 18 Mar. 2025.

16. **Disney+.** “Subscriber Agreement.” ***Disney+.*** Accessed 18 Mar. 2025.

17. **Disney+.** “Disney Privacy Policy.” ***Disney.*** Accessed 18 Mar. 2025.

18. **eBay.** “User Agreement.” ***eBay.*** Accessed 18 Mar.

2025.

19. **eBay.** “User Privacy Notice.” ***eBay.*** Accessed 18 Mar. 2025.

20. **Epic Games.** “Terms of Service.” ***Epic Games.*** Accessed 18 Mar. 2025.

21. **Epic Games.** “Fortnite End User License Agreement.” ***Epic Games.*** Accessed 18 Mar. 2025.

22. **Facebook (Meta).** “Terms of Service.” ***Facebook.*** Accessed 18 Mar. 2025.

23. **Facebook (Meta).** “Data Policy.” ***Facebook.*** Accessed 18 Mar. 2025.

24. **Flickr (SmugMug).** “Terms of Use.” ***Flickr.*** Accessed 18 Mar. 2025.

25. **Flickr (SmugMug).** “Free Accounts & Storage Limits.” ***Flickr.*** Accessed 18 Mar. 2025.

26. **GitHub (Microsoft).** “Terms of Service.” ***GitHub.*** Accessed 18 Mar. 2025.

27. **GitHub (Microsoft).** “Privacy Statement.” ***GitHub.*** Accessed 18 Mar. 2025.

28. **Google.** “Terms of Service.” ***Google.*** Accessed 18

Mar. 2025.

29. **Google.** “Privacy Policy.” ***Google.*** Accessed 18 Mar. 2025.

30. **Google.** “Gmail Program Policies.” ***Google.*** Accessed 18 Mar. 2025.

31. **Google.** “YouTube Terms of Service.” ***YouTube.*** Accessed 18 Mar. 2025.

32. **Google.** “YouTube Community Guidelines.” ***YouTube.*** Accessed 18 Mar. 2025.

33. **Google Play.** “Google Play Terms of Service.” ***Google Play.*** Accessed 18 Mar. 2025.

34. **Hulu (Disney).** “Terms of Use.” ***Hulu.*** Accessed 18 Mar. 2025.

35. **Hulu (Disney).** “Privacy Policy.” ***Hulu.*** Accessed 18 Mar. 2025.

36. **IBM.** “Cloud Services Agreement.” ***IBM.*** Accessed 18 Mar. 2025.

37. **IBM.** “IBM Privacy Statement.” ***IBM.*** Accessed 18 Mar. 2025.

38. **Instagram (Meta).** “Terms of Use.” ***Instagram.*** Accessed 18 Mar. 2025.

39. **Instagram (Meta).** “Data Policy.” ***Instagram.*** Accessed 18 Mar. 2025.

40. **LinkedIn (Microsoft).** “User Agreement.” ***LinkedIn.*** Accessed 18 Mar. 2025.

41. **LinkedIn (Microsoft).** “Privacy Policy.” ***LinkedIn.*** Accessed 18 Mar. 2025.

42. **Lyft.** “Terms of Service.” ***Lyft.*** Accessed 18 Mar. 2025.

43. **Lyft.** “Driver Agreement.” ***Lyft.*** Accessed 18 Mar. 2025.

44. **Mastercard.** “Terms of Use.” ***Mastercard.*** Accessed 18 Mar. 2025.

45. **Mastercard.** “Global Privacy Notice.” ***Mastercard.*** Accessed 18 Mar. 2025.

46. **Medium.** “Terms of Service.” ***Medium.*** Accessed 18 Mar. 2025.

47. **Medium.** “Rules.” ***Medium.*** Accessed 18 Mar. 2025.

48. **Microsoft.** “Microsoft Services Agreement.” ***Microsoft.*** Accessed 18 Mar. 2025.

49. **Microsoft.** “Microsoft Privacy Statement.”

Microsoft. Accessed 18 Mar. 2025.

50. **Microsoft.** “Teams Terms of Use.” ***Microsoft.*** Accessed 18 Mar. 2025.
51. **Mozilla.** “Firefox Privacy Notice.” ***Mozilla.*** Accessed 18 Mar. 2025.
52. **Netflix.** “Terms of Use.” ***Netflix.*** Accessed 18 Mar. 2025.
53. **Netflix.** “Privacy Statement.” ***Netflix.*** Accessed 18 Mar. 2025.
54. **Netflix.** “Arbitration Agreement (U.S.).” ***Netflix.*** Accessed 18 Mar. 2025.
55. **Nintendo.** “Nintendo eShop Terms of Service.” ***Nintendo.*** Accessed 18 Mar. 2025.
56. **Oracle.** “Oracle Cloud Hosting and Delivery Policies.” ***Oracle.*** Accessed 18 Mar. 2025.
57. **PayPal.** “User Agreement.” ***PayPal.*** Accessed 18 Mar. 2025.
58. **PayPal.** “Acceptable Use Policy.” ***PayPal.*** Accessed 18 Mar. 2025.
59. **Pinterest.** “Terms of Service.” ***Pinterest.*** Accessed 18 Mar. 2025.

60. **Pinterest.** “Privacy Policy.” ***Pinterest.*** Accessed 18 Mar. 2025.

61. **ProtonMail (Proton AG).** “Terms and Conditions.” ***ProtonMail.*** Accessed 18 Mar. 2025.

62. **Reddit.** “User Agreement.” ***Reddit.*** Accessed 18 Mar. 2025.

63. **Reddit.** “Privacy Policy.” ***Reddit.*** Accessed 18 Mar. 2025.

64. **Salesforce.** “Master Subscription Agreement.” ***Salesforce.*** Accessed 18 Mar. 2025.

65. **Salesforce.** “Privacy Statement.” ***Salesforce.*** Accessed 18 Mar. 2025.

66. **Shopify.** “Terms of Service.” ***Shopify.*** Accessed 18 Mar. 2025.

67. **Shopify.** “Acceptable Use Policy.” ***Shopify.*** Accessed 18 Mar. 2025.

68. **Signal Messenger.** “Terms & Privacy Policy.” ***Signal.*** Accessed 18 Mar. 2025.

69. **Slack (Salesforce).** “Customer Terms of Service.” ***Slack.*** Accessed 18 Mar. 2025.

70. **Slack (Salesforce).** “Privacy Policy.” ***Slack.***

Accessed 18 Mar. 2025.

71. **Slack (Salesforce).** “Workspace Data Export Policy.” ***Slack.*** Accessed 18 Mar. 2025.

72. **Snap Inc.** “Snapchat Terms of Service.” ***Snapchat.*** Accessed 18 Mar. 2025.

73. **Snap Inc.** “Snapchat Privacy Policy.” ***Snapchat.*** Accessed 18 Mar. 2025.

74. **Sony.** “PlayStation Network Terms of Service and User Agreement.” ***Sony.*** Accessed 18 Mar. 2025.

75. **Sony.** “Privacy Policy.” ***Sony.*** Accessed 18 Mar. 2025.

76. **Spotify.** “Spotify Terms and Conditions of Use.” ***Spotify.*** Accessed 18 Mar. 2025.

77. **Spotify.** “Privacy Policy.” ***Spotify.*** Accessed 18 Mar. 2025.

78. **Steam (Valve).** “Steam Subscriber Agreement.” ***Valve.*** Accessed 18 Mar. 2025.

79. **Telegram.** “Terms of Service.” ***Telegram.*** Accessed 18 Mar. 2025.

80. **Telegram.** “Privacy Policy.” ***Telegram.*** Accessed

18 Mar. 2025.

81. **Tesla.** “Connected Car Services Terms of Use.” ***Tesla.*** Accessed 18 Mar. 2025.

82. **Threema.** “Terms of Service.” ***Threema.*** Accessed 18 Mar. 2025.

83. **Tinder (Match Group).** “Terms of Use.” ***Tinder.*** Accessed 18 Mar. 2025.

84. **Tinder (Match Group).** “Privacy Policy.” ***Tinder.*** Accessed 18 Mar. 2025.

85. **Tumblr (Automattic).** “Terms of Service.” ***Tumblr.*** Accessed 18 Mar. 2025.

86. **Tumblr (Automattic).** “Community Guidelines.” ***Tumblr.*** Accessed 18 Mar. 2025.

87. **Twitter (X Corp.).** “Terms of Service.” ***X.*** Accessed 18 Mar. 2025.

88. **Twitter (X Corp.).** “Privacy Policy.” ***X.*** Accessed 18 Mar. 2025.

89. **Uber.** “Terms and Conditions.” ***Uber.*** Accessed 18 Mar. 2025.

90. **Uber.** “Privacy Notice.” ***Uber.*** Accessed 18 Mar. 2025.

91. **Uber Eats.** “Additional Terms for Eaters.” ***Uber.*** Accessed 18 Mar. 2025.

92. **Venmo (PayPal).** “User Agreement.” ***Venmo.*** Accessed 18 Mar. 2025.

93. **Vimeo.** “Terms of Service.” ***Vimeo.*** Accessed 18 Mar. 2025.

94. **Vimeo.** “Privacy Policy.” ***Vimeo.*** Accessed 18 Mar. 2025.

95. **Waze (Google).** “Terms of Use.” ***Waze.*** Accessed 18 Mar. 2025.

96. **Waze (Google).** “Privacy Policy.” ***Waze.*** Accessed 18 Mar. 2025.

97. **WhatsApp (Meta).** “Terms of Service.” ***WhatsApp.*** Accessed 18 Mar. 2025.

98. **WhatsApp (Meta).** “Privacy Policy.” ***WhatsApp.*** Accessed 18 Mar. 2025.

99. **OkCupid (Match Group).** “Terms of Use” and “Privacy Policy.” OkCupid. Accessed 18 Mar. 2025.

100. **Coinbase.** “User Agreement.” Coinbase. Accessed 18 Mar. 2025.

WE SHAPE OUR TOOLS, AND THEREAFTER OUR TOOLS SHAPE US.

Marshall McLuhan

RED ZONE MANUALS ARE AVAILABLE ON LUTAV.CO/RED

A Red Zone Manual is that subtle alarm telling you we're only five minutes into the future—where something feels off, but not enough to make you scream.

Conceived with design principles and futures foresight methodology, each manual is a practical field guide to the hidden pitfalls in our everyday systems, shining a light on realities that quietly shape our freedoms and choices.

Red Zone Manuals aim to give you a clear, concise look at looming threats so you can decide what to do before the sirens start blaring—because by then, it may already be too late.