ChangeThis
185.03


# A DECLARATION OF CITIZEN-USER RIGHTS

Alexis Wichowski

# The smartphone didn't just make life easier; it didn't just make us, as Apple's '90s-era slogan urged, "think different." It made *life* different.

Today, tech entities are no longer simply making spreadsheet software and calendar apps and gadgets. They are battlefields. They are Weapons. The problem here is that no one knows what to call these new things. As I first introduced in a 2017 *WIRED* article, I propose that we call them "net states."

Why not just keep calling them "the tech industry"? The short answer is that the tech industry is no monolith, with all its companies pursuing the same goals with the same business practices.

As hard as it may be to think of the world's newest industry as traditional in any way, a handful of "traditional" companies have undergone a metamorphosis. And, in the same way we don't keep calling butterflies "caterpillars" once they've transformed, these particular companies—Amazon, Apple, Facebook, Google, Microsoft, and Tesla, specifically—have morphed into something altogether different from "the tech industry."

They no longer only make products and offer services. They're reaching beyond their core technologies to assert themselves in our physical world. They're inserting digital services into our lived environments in ways both unseen and, at times, unknown to us. And, most important, they're exerting formidable influence over the way our world works on individual, societal, and geopolitical levels. These tech companies are unlike anything we've encountered before.

These net states vary in size and structure but generally exhibit four key qualities: They enjoy an international reach. Their core work is based in technology. Their pursuits are influenced, to a meaningful degree, by beliefs, not just a bottom line. And, perhaps most significant, they're actively working to expand into areas formerly the domain of governments, areas that fall outside their primary products and services—areas they pursue at times separate from and even above the law.

Today, tech entities are no longer simply making spreadsheet software and calendar apps and gadgets. They are battlefields. They are Weapons.

Simply put, net states are not just out to make widgets or get people hooked on a single product. (This is why I believe Tesla—with its world-building businesses—is a net-state, and Twitter, with its single, stand-alone platform, is not.) Net states are out to change the world—not just in theory, but in defense, diplomacy, public infrastructure, and citizen services. Net states are tech entities that act like countries. By acting like countries, net states alter our experiences as citizens. And they alter countries' experiences as geopolitical powers.

Net states matter because they provide us with the tools to enhance our sense of freedom—the one thing we've really got going for us. But, just because they make us feel free doesn't mean that they don't come with a cost. We are empowered by the devices that give us the world's answers at the touch of our fingertips. Yet we feel powerless to do anything about what personal information is collected in the process. We are empowered by our incredible increase in awareness about what's going on in the world, thanks to the massive amounts of media we consume each day. But we feel powerless to do anything to stem the tide of terrible things we read and hear about. We are, in feeling and in fact, more cognitively powerful—we can see more, find more, learn more, connect more—than we've ever been at any point in our history. Yet we're paralyzed, unable to engage in meaningful action; our attention is drained, our bandwidth exceeded; our emotions and cognition are overloaded and exhausted.

We can't persist like this. The more media we expose ourselves to through technology, the more we feel beaten down by the incivility we see in partisan politics—in Washington, DC, yes, but also among the acquaintances in our social networks.

Take, as just one example, Russian misinformation warfare during the 2016 election. We know more about it than we ever could have, pre-social media. Yet we don't see action on the part of our elected leaders to protect the 2020 election from similar warfare. And we don't feel as if we can do anything about it on our own. We're also in the midst of what feels like an endless war on terror—multiple wars, if you count the onslaught of cyberattacks on our country: 4,000 a day, according to the FBI.

It's almost impossible to conceptualize it all, let alone feel as if we can be part of the fight.

There's no silver bullet for our problems. We can't fix all the world's ills. But some component of our sense of powerlessness lies with our (simultaneously empowering) technology, and I do have a suggestion to address that.

We do not need to feel powerless. We are not, in fact, powerless. We need to remind ourselves and the keepers of our digital realm of that. We need, as once in a while the world seems to need, a declaration: a set of suggestions that establish ground-floor, foundational conditions that should apply to every human being on Earth.

We need to establish a new relationship with our net states—one that reclaims power that users can exert over their own data, their sense of privacy, and their experiences of the digital ecosystem. We need a pact that puts citizen-users at the center—a digital descendent of the Universal Declaration of Human Rights, a tech-savvy version of the Constitution's Bill of Rights. We don't need any more terms of service. We don't need Bible-length provisions to counter the unreadable terms net states provide us. We need just a few basic principles—brief but unassailable fundamentals that everyone should be assured. We need a Declaration of Citizen-User Rights.

The goal of such a pact—not an agreement that net states write and users must accept, but rather an agreement that citizen-users craft, enumerating rights we expect to be respected—is to create a set of ground rules that net states must agree to in exchange for our using their products: specifically, in exchange for our data and our attention.

To figure out how to create such a pact, we can look to several precursors, road maps for what a meaningful pact between net states and users could look like. The Cybersecurity Tech Accord (aka the Digital Geneva Convention) signed by more than 80 global companies may seem like a likely candidate. But for all its laudable qualities, it's actually not the best model for what citizen-users need for their protections among net states. The Digital Geneva Convention gets a lot right. But the main issue is that it's not really for users. It's a pact by net states for net states. Users are among the objects of the pact, but they're not really a party to it; only the net states are.

We don't need any more terms of service. We don't need Bible-length provisions to counter the terms net states provide us. We need just a few basic principles.

Before we can craft a user-centric declaration, let's quickly review the current state of affairs with what we've already signed on to.

Everyone who uses technology is already party to multiple versions of terms of service (TOS). But these, too, aren't for us; they're for tech companies to protect themselves from liabilities. They're the gate through which we must pass to use a company's products and services. So we agree to them, time and again, without reading them. Even if we did read them, we'd discover that they don't put us—the users—and our protections front and center. The focus is on the tech company itself, ensuring that it doesn't get sued when it eventually shares your data with third parties.

There are various websites that attempt to help users navigate which platforms and services have TOS that are more or less risky for the user. For example, the website Terms of Service; Didn't Read, or TOSDR (a play on "too long; didn't read," generally shortened to TLDR, which refers to online content that people caution they didn't bother reading), was launched in 2012 in collaboration with the Electronic Frontier Foundation (EFF). It classifies sites depending on their risk to users, from A to E. (The search engine DuckDuckGo gets an A since it doesn't keep track of search queries; YouTube gets a D, mostly because it keeps deleted videos for its internal purposes, unknown to the user who created the content.) The rating of TOS is a collaborative effort: users from all over the web note changes to TOS on GitHub, one of the most widely used code-sharing platforms. But this also means it's uneven—without armies of online volunteers, it's difficult to assess how "good" TOS are for users. TOSDR does helpfully compile various TOS into a single location with plain-language summaries. Even if out of date and far from exhaustive, its list is still quite instructive (as are those of other sites).

To see if I could flesh out what was missing on TOSDR, in August of 2018, I compiled and read all the terms of service for Amazon, Apple, Facebook, Google, Microsoft, and Tesla. Here's what I found.

First, there's a wide range of "average" when it comes to the sheer length of terms of service. (Note: for the purposes of this exercise, I examined only language explicitly called "terms of service"—not ancillary policies, such as those mentioned in FAQ or other legal policies listed; in other words, I stuck to the agreement between the user and the platform or service.)

Apple's iTunes TOS section is a handful, adding up to around 6,804 words. Google embraces brevity (and ambiguity—more on that shortly), with its TOS clocking in at about 1,869 words. Facebook is somewhere in the middle, at 3,243 words. Amazon is about the same, at 3,387. Microsoft blasts the others out of the water for length, at 15,290 words. Tesla covers their business in 5,736 words. All this averages out to terms of service composed of 7,265.8 words for your standard net state. Even if these terms were written in plain English, as many of them now are (thanks to the need to comply with the EU's General Data Protection Regulation), if the average person reads 200 words per minute, it would take 36 minutes to read one single platform's terms of service; 3 hours and 20 minutes for all the ones I calculated—just six of zillions.

In practice, we not only don't want to spend this much time reading TOS, we come across too many to realistically do so. Researchers at Carnegie Mellon University estimated that we encounter 76 sets of terms of service in a year, based on our 2008 browsing habits26—back when we spent only 13 hours a week, or 1.8 hours a day online. Terms of service are shorter now—again, thanks to the EU's GDPR. But we're still encountering them quite regularly. In 2016, it was estimated that we spent 10 hours and 39 minutes per day con-

suming media in some form—via our smartphones, TVs, computers, tablets, e-readers, and so on. Our attention is a precious commodity. We try hard not to waste it; we spend only 10 to 20 seconds per web page to evaluate whether it's worth our time before moving on to the next one.

If we can barely pay attention for the 10-plus seconds it takes to see whether or not we want to stay on a web page, the notion that we'd take 36 minutes to peruse a boring user agreement—76 times a year, no less—is simply unrealistic.

And our net states in question? There are six that I mentioned above. But they're not just six companies; they're six parent companies, and collectively they've acquired 673 other companies, according to transaction data publicly available through Crunchbase. Many of the acquired entities are likely irrelevant to us: Apple bought lots of hardware component manufacturers, for instance; Facebook, lots of messaging startups. But many of them are significant entities that we run into on occasion, though we may not be aware that they're owned by a major net state: Instagram and WhatsApp (owned by Facebook); Skype, LinkedIn, and Nokia (those are Microsoft's); IMDb and Zappos (Amazon bought those); YouTube, Waze, and Zagat (all Google's), to name just a few. And they all have their own terms of service as well. Indeed, if we were to map out the universe of the net states and their 673 acquisitions, I'm fairly certain we'd discover that there's no way to both be active in the digital sphere and avoid having to agree to terms of service informed by one of the major net states.

In sum, if we're online, we are bound to our net states, in some way. We've given ourselves over to them, without even knowing what that really means. We can't put this particular genie back in the bottle—the data we've set free has likely passed through so many third parties at this point that it would be virtually impossible to suck it all back in. But we can

make a decision to change how we handle our data moving forward, to reclaim power over what we give out, to whom, and for what purposes.

Let's start practically. Here are the major areas covered in the big-six net state terms of service: (1) your data when you use their product/service; (2) your data once you leave their product/service; (3) your expectation of privacy while using their product/ service; (4) the ground rules about using their product/service; and (5) what access third parties have to your data.

The reason to start with existing areas in the terms of service is that the ultimate goal for crafting a Declaration of Citizen-User Rights is to be a viable challenge to the TOS that net states create. Thus we can't ignore their areas of concern. But instead of focusing on ensuring that the net states don't get sued, our document—a set of universal "terms of rights"—will ensure that citizen-users don't get taken advantage of.

We can make a decision to change how we handle our data moving forward, to reclaim power over what we give out, to whom, and for what purposes.

First, some general observations on terms of service. Based on those that I examined, they tend to be an umbrella set of conditions users must agree to. Yet despite their length, they don't come close to laying out all the details—especially some of the details users are likely most concerned with. For example, all six net state TOS that I reviewed directed readers to a separate "Privacy Policies" document that users were encouraged, but not required, to read. These are the policies that really get into detail about what they're doing with our data. By including a blanket statement in the TOS along the lines of "By accepting this agreement, you're also accepting our privacy policies, which you can read here [click here]," companies effectively shuttle their privacy policies even further out of users' reach.

I'll spare you the mind-numbingly boring details. Here's the upshot, which isn't great news but no surprise: if you use any product or service of the six major net states, you don't really have any privacy online. Your data will be kept, analyzed, and shared with or sold to third parties, as they see fit. One notable exception is Apple, sometimes: whatever data is on your phone remains on your phone, not on Apple servers—unless you enable automatic syncing with iCloud. This is one of the reasons iPhones bedevil law enforcement officials: there's no "back door" where Apple can unlock someone's phone, remotely or in person. If you use a strong password—meaning, not the word "password" or "1 2 3 4 5 6," which remain the two most common passwords, amazingly—it's really, really hard for anyone to break into your phone.

The data collected while using your phone is all tracked of course. Facebook notes, for instance, "We use the data we have—for example, about the connections you make, the choices and settings you select, and what you share and do on and off our Products—to personalize your experience." This means that if you have Facebook open on your

phone and then open another app, Facebook will collect data on what you're doing on that app, too. All the net states (and tons of other companies, too) share or sell—also called "licensing"—your data with unnamed "third parties" as they see fit, for which you have granted them "worldwide" permission, according to their TOS. Amazon goes so far as to say that they'll also share or license your name in addition to your data, if you've ever posted a review or comment.

In short, our data online is pretty exposed. We say we care a lot about it—a Pew poll in 2016 reported 75 percent of us as saying privacy is "very important" to us. But we do precious little to actually protect our privacy online. Almost all of us—91 percent—accept TOS without reading them (the figure is closer to 97 percent for millennials). Claiming to care about privacy but not taking action to protect it is such a widespread phenomenon that researchers have dubbed it the "privacy paradox." The most plausible explanation I've seen for this paradox has to do with our squishy sense of time. Our worries about privacy—a breach, a leak, an abuse of our data—are focused on something possibly happening in the future. The future's an abstract concept; it's difficult to visualize in a tangible way. On the flip side, the actions that put our privacy at risk are in the now. We're getting something immediately—access to information, a platform or service, the ability to connect, see photos, receive updates. We get visceral, tangible, right-now representations of our friends, our frenemies, our crushes, our curiosities. All you have to do is sign away your privacy with the click of a TOS "accept" button and bam! You're in; you're connected to the object of your desire, whatever that may be. But taking the time to be careful about your privacy takes, well, time—a lot of it—as well as that prized commodity, your attention.

So here's what I propose: we take the time to negotiate a better deal for ourselves. Let's set out a few simple, high-level terms that protect users. Our focus in the Declaration of Citizen-User Rights is to address the meat of the problem: how to reclaim the right to our privacy—and our sense of power—without having to sacrifice the benefits of technology.

The goal with these rights is not to codify tactics for user protection against technology's ill effects—for example, steps to turn off location-tracking on your phone or to prevent your contacts list from being uploaded without your permission. For these sorts of protections, the Center for Humane Technology, founded by former Silicon Valley leaders, provides excellent resources. The goal here is to identify the fundamental rights that users would need to claim to substantively alter the balance of power between us and net states.

Instead of focusing on ensuring that the net states don't get sued, our document —a set of universal "terms of rights"— will ensure that citizen-users don't get taken advantage of.

There are likely dozens of possible rights. Let's start, though, with the three rights poised to make the greatest impact on our lives, expressed here as three principles. Those principles alone make up the Declaration of Citizen-User Rights. They are:

1. **Citizen-users have the right to choose how they pay for their own content privacy.**

2. **Citizen-users have the right to delete their own content from the public record.**

3. **And citizen-users have the right to know how their data is being used.**

I go into greater detail on what these rights entail in my new book, *The Information Trade*. What they are predicated upon is the current reality that, with respect to our own content and net states, we're not currently in a state of equilibrium. We're not getting out as much as we're putting in. Our content goes to net states, and then disappears behind their fire-walls. We can't see it all assembled. It goes into databases that generate insights—insights about our behaviors and habits and preferences—that net states gain benefits from but that we—the creators of the data—don't necessarily know about and certainly don't have access to.

This has to change. And we—the citizen-user content creators, the creatures who populate the digital ecosystem with our thoughts, our memories, our records, and our interactions—already have the power to ensure that it does change.

Without us, the digital ecosystem loses its life force. Websites absent of users interacting with them are virtual ghost towns, with no data to gather and analyze. We, the citizen-users, provide the energy that fuels the ecosystem; the net states provide only the space and pathways within it. So if we want our Declaration of Citizen-User Rights adopted, we

have to use our power to withhold information from a website; to boycott usage; switch to a different service or platform that will agree to our terms and respect our rights. We can massively disrupt the equilibrium of the digital ecosystem, should we so desire. We just have to commit to doing it.

In short, it is in the best interests of all parties to the digital ecosystem to ensure that its human population is cared for. We don't need to deny ourselves the benefits that tech provides us. As *New York Times* "Smarter Living" editor Tim Herrera reflected, "When we talk about un-plugging, I think what we're really talking about is structuring our lives in ways that allow technology to serve us, rather than the other way around."

Right now, we serve tech companies—we give them our data, they generate insights based on that data, and we never see the results. We can continue to supply tech companies our data, but under different conditions—conditions, laid out in the Declaration of Citizen-User Rights, that give us control over and information about that data. We don't need to unplug and retreat from tech. We just need to adjust the equilibrium in the digital ecosystem.

In short, we need new rights in these new net states. Rights bring power. They are our protection against potential abuses of power. They are, according to the US Constitution, inviolate—something we're born with as Americans. And we are fortunate to have those rights. As Hannah Arendt, a philosopher who was stateless for 17 years, once wrote, "The right to have rights, or the right of every individual to belong to humanity, should be guaranteed by humanity itself." She then added, "It is by no means certain whether this is possible."

Net states, operating internationally, have the opportunity to afford their users rights that may differ from and even exceed rights of any individual's nation-state (or, for the currently 10 million stateless people in the world, stand in place of citizenship rights). In this way, the rights afforded by net states rise above those guaranteed by nation-states.

The nation-state is no longer the only game in town. Nation-states can partner with net states, as they have in the partnerships between Tesla and Vermont, California, and Connecticut. They can establish contracts with net states, as the federal government does in operating almost entirely on net state technology. Conversely, they can fight against net states: with regulations, as in the EU; with taxes, as in Uganda; or with bans, as in Papua New Guinea and Sri Lanka.

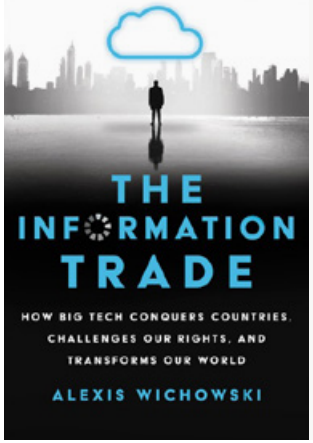
Whatever type of relationship nation-states and net states ultimately have, the reality is that there must be some sort of a relationship—and it must be diplomatic in nature, not just economic. As things now stand, net states don't have just our information; they also

We can massively disrupt the equilibrium of the digital ecosystem, should we so desire. We just have to commit to doing it.

have power over our rights. If nation-states don't set the terms of how net states must operate with respect to our rights, then net states will write their own rules of engagement, in some cases avoiding regulations, as Facebook did when it moved more than a billion users out of its data center in Ireland—or adapting to them, as Google and Apple have done to comply with the GDPR.

We—as citizens and citizen-users—have the right to have rights: with our nation-states and with our net states. It is up to our home coun-tries to enforce the rights they've granted in our constitutions. And it is up to us as individuals to hold our net states accountable if they fail to grant us protection with respect to those rights. The US Constitution holds that we have the right to "be secure in [our] persons, houses, papers, and effects." **Our data may not be who we are, but it is certainly something of us. As such, it is something that needs to be secured.**

# Info




Ready to dig deeper into this idea?
Buy a copy of
The Information Trade.

Want copies for your organization or for an event? We can help:
customerservice@porchlightbooks.com 800-236-7323

## ABOUT THE AUTHOR

Alexis Wichowski is the deputy chief technology officer for the City of New York, and an adjunct professor of technology, media, and communications at Columbia University. A widely recognized technology expert, Wichowski spent the past two decades working at the intersection of technology, media, and government, most recently at the State Department and the United Nations. Her work has appeared in *The Atlantic*, *TechCrunch*, *Foreign Affairs*, and *Wired*, which published her viral piece, "Net States Rule the World: Ignore Them at Your Peril."

**SHARE THIS**

Pass along a copy of this manifesto to others.

**SUBSCRIBE**

Sign up for e-news to learn when our latest manifestos are available.

**Porchlight**

Curated and edited by the people of Porchlight, ChangeThis is a vehicle for big ideas to spread. Keep up with the latest book releases and ideas at porchlightbooks.com.

This document was created on February 19, 2020 and is based on the best information available at that time.