HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

POLICY PAPER
belfercenter.org/homelandsecurity

HOMELAND SECURITY PROJECT | MAY 2023

# Reach, Choice, and Transparency*

## Governing the Internet in the 21st Century

Steve Johnson

# Executive Summary

As inventions go, the Internet stacks up with the best of them: the lightbulb, the automobile, even fire. In its first thirty years, the Internet's worldwide adoption and breadth of application has exceeded any other technological advance in history. It expands our reach by bringing people, experiences, and things to us with the click of a mouse. It connects us to an increasing number of gadgets, from smartphones to voice kiosks and soon self-driving vehicles that will no doubt converse with us while we commute, happily oblivious to the traffic around us. We revel in our newfound agility and versatility. Importantly, our precious network kept us sane during a worldwide pandemic and enabled the world to work remotely while most of its population was frozen at home. For resilience against catastrophes alone, the Internet has become indispensable.

* This essay is based on a book the author is currently writing on Internet regulation.

But while our digital revolution has unquestionably improved our lives, has it made us freer? We have more choices, but are we better equipped to choose? Or rather, is this cyber world to which we're steadily migrating a place where projections replace tangible things with little permanence or authenticity that hobble our ability to perceive, think, and judge? Are we slowly embedding ourselves in an environment where our instincts are less effective, where, after eons of evolution, our native ability to govern our lives is weakened or disabled?

This is the central question of our age. How does the Internet affect our power to manage our lives: first, our control over the things that surround us – our *reach*; second, our faculty for soundly *choosing* from those things what to do, consume, or engage with; and third, our ability to grasp and understand – to *know* – what we have chosen, so that we can enjoy, act, or believe based upon grounded truth?

As our lives become more entwined with the electronic provision of things – including relationships with others – policymakers must ensure that on the Internet, citizens can continue to mostly *self-govern* as they have in all the countless permutations of societies across the ages. Self-governance entails the ability to manage our affairs with minimal supervision. Even in the most despotic regimes, individuals can comprehend their environment and make judgments to manage their day-to-day activities. Any human society would fail without this necessary degree of individual autonomy – not only for personal liberty's sake, but for practical reasons. There are far too many activities to manage otherwise.

As more and more of society's critical functions go digital, government must see as its primary regulatory responsibility protecting individual agency, namely people's ability to perceive, judge, and trust or distrust the things with which they interact. The Internet may be putting these prerequisites of self-governance to their toughest test ever.

# Background

In 1992, when Sir Tim Berners-Lee blessed us with a new medium he presciently dubbed the Web (as in "Oh, what a tangled…"), we welcomed a new age of freedom. After all, this collection of clickable links removed friction, interconnected the globe, and all but erased gravity. It moved us *at the speed of light* to practically any point on Earth. It was a means of communication and a brand-new mode of transport. Three decades later, it carries us to doctor's appointments, shopping malls, cinemas, and, especially, to each other countless times a day.

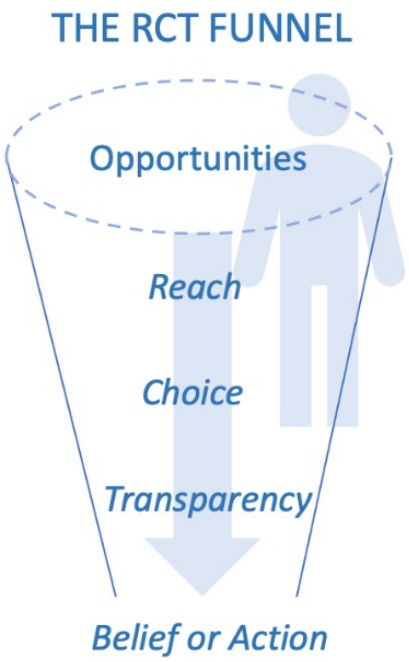
But as it grew from a corner chat room and information repository to the very substrate of society, we lost sight of its peculiar curse: this virtual place isn't the world as we know it. Instead, our new home on the Web is like a cross between the wild west town of Deadwood and the fabricational world of the Metaverse. Yet, on a social evolutionary timescale, our migration has been as quick as a stampede. Before long, everyone on earth will be wired to a frontier we've barely begun to tame.

Today, public attention on Internet regulation focuses on incipient threats – every year sees another rising concern, whether of child predation, cult radicalization, or AI world domination. Many of these fears are valid and must be addressed. Yet bringing safety to the Internet requires a much larger lens – indeed, an anthropological one. Piecemeal remedies won't safeguard the Internet. Instead, it needs a framework for restoring the human senses and laws of nature, as it were – permanence, authenticity, and protectible boundaries – so that people can navigate and interact electronically as confidently as they have for centuries on terrestrial Earth. The very technologies we fear – large language models, for example – could, if properly harnessed, provide tools for assuring even more safety in cyberspace than we experience elsewhere. But neither users, government, nor the market have diagnosed the cultural threat well enough to harness our breakthrough inventions to restore order.

# An Algorithm for Regulation

If we aim to ensure people can set and protect their space, make informed choices, and understand what they choose (so they're not routinely fooled), then we need a framework that fits those three activities. In this age of algorithms, let's look at our modus vivendi as an algorithm. Consider the following.

Let's call the breadth of our lives our **Reach**. It is our wholesale cut, marking the perimeter of our opportunities. For example, it's our town, place of worship, news sources, family, and friends. Our reach defines what we encounter daily, which we try to curate to the degree possible to include what we prefer and exclude what we abhor.




**Choice** is our manner of winnowing our opportunities to the few we want to consider and picking which to seize. (Daniel Kahneman might call this fast and slow thinking.) We peruse our alternatives to estimate what's inside, selecting and filtering based on the packaging, appearance, name, or history, using our prior knowledge or trusted sources as a guide. Our success – choice of news story, conversation, or product, for instance – will depend on how well we can predict based on surface information.

Once we engage, our experience is determined by the **Transparency** of what we receive. Transparency refers to the whole experience, including the qualities of the person or activity and the context and history that complete the picture. Nothing is entirely self-evident or self-contained; we need all the elements, internal and external, past and present, to fully appreciate and comprehend any experience. Information will always be incomplete, but more transparency is better.

The Reach, Choice, and Transparency algorithm – our RCT model – describes people's approach to accessing the world. It's a framework for the three pillars of effective self-governance. While it may seem complex, we need all three for complete control. If we look narrowly at only choices in the moment – for example, whether a news article is factual, product is accurately labeled, or an ad contains harmful information – we ignore the upstream processes that brought us to those choices. This is why democracies place importance on freedom of choice but also of opportunity. Occlusions higher up our experiential journey will constrain, bias, or trap us in a limited set

of options inferior to others we might prefer. If we can't manage our reach, then any choice in the moment isn't as free as it may appear. Thus, Internet regulators must tend to the well-functioning of the entire RCT. They need to ensure people can select and filter their environment (Reach), navigate their alternatives (Choice), and accurately process what they choose (Transparency).

~

Our RCT works on terrestrial Earth because human instincts are well-adapted to the tangible world. We perceive things directly and can count on them to be stable and predictable. Reliable appearances and consistent behavior facilitate our mind's simulation. Therefore, we can curate our environment by watching, judging, choosing, and dodging with reasonably good results. When we encounter other people, there is a symmetry between us that enables us to gauge trust. Thus, physical law, our senses, and our inductive brains help us learn what's good for us with minimal mistakes.

The Internet plays havoc with this arrangement. Cyberspace flattens the Earth to two dimensions, reduces people's senses to a monitor and mouse, and throws identity, permanence, and authenticity out the window. We know things not by sight or smell but by their labels. Cues to meaning and trustworthiness, such as context and track record, are unreliable or absent. The Internet supplies porous perimeters, misleading signage, and transitory people and things. And, unlike our advanced non-digital societies, ethical or legal recourse is nearly absent. By 21st-century standards, cyberspace is still barbaric.

The trouble is, we've wandered into this wonderland without fully realizing our predicament – perhaps because of how quickly we've migrated. Now that we've arrived, we assume community will function just as well electronically as it does terrestrially. Consequently, we keep shifting our activities to the Web, coveting the openness we construe as freedom. We're now sensing danger, so regulators are rushing to counter the obvious breakdowns, scrambling, for instance, to alleviate privacy concerns with data restrictions and fakery by insisting on manual content moderation. But breaches of privacy and responsibility are only markers of a place where certainty and accountability are too scarce for comfort. These policies attend to bad cyber behavior without mending cyber society itself.

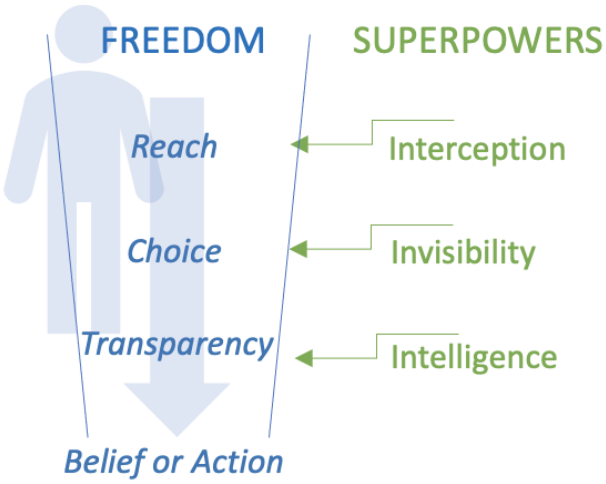
# The Internet's Superpowers

We have invented an alien environment that lacks the prerequisites for self-governance human societies have always possessed. The Internet blunts our acumen for bracketing, assessing, and experiencing the world. But there's more. Frighteningly, cyberspace confronts us with *concerted* forces—powers harnessed by others—that can completely undermine the RCT.

Imagine the disruption to self-governance if comic book superpowers existed – say, teleportation, shapeshifting, and mind-reading. If such powers existed in the real world, we'd already have convened a dozen constitutional conventions to devise detections, shields, antidotes, and laws to rein them in. Well, these fairy tale superpowers have already arrived on the Internet.

Anyone with a credit card can harness the Internet's platforms (Google, Facebook, Apple, and others) to intercept other users at will, use data-fed intelligence to mislead them, wield false authority with an assumed name, and then vanish. I call these cyber powers *Interception*, *Invisibility*, and *Intelligence*.

**Interception**, like teleportation, is the ability to insert oneself into someone else's space without permission—threatening Reach. The closer and more intimate our devices, the easier the Interception.



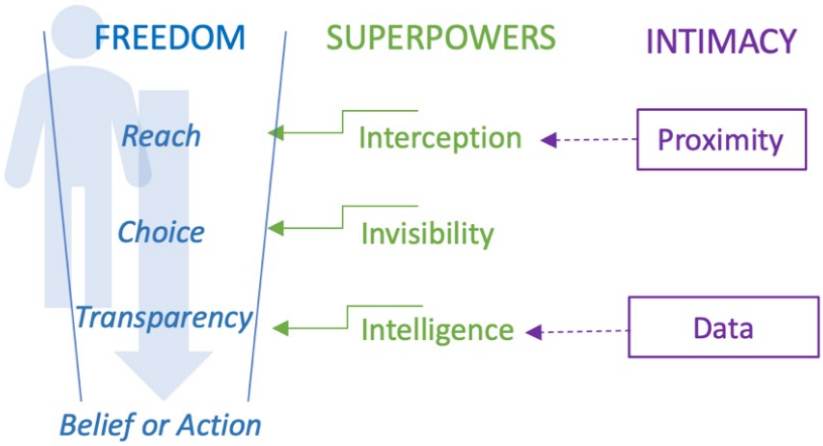

**Invisibility**, like shapeshifting, is the ability to change identities at will—threatening Choice. The Internet provides unlimited aliases (account names, email addresses, dating handles, and so on) at little cost. Today, there is no accepted way to authenticate identity, linking them across applications, or guaranteeing they will last.

**Intelligence**, like mind-reading, is the awareness of someone's whereabouts and intentions, which can be used to find and influence them—threatening Transparency. Data-collecting applications and devices fund the Intelligence superpower.

Our human powered RCT is no match for these cyber powers. When strangers can freely enter our space, shift to any identity, and know us better than we know ourselves, our online lives

become a dream where trust in people and things has no purchase. Surrounded by super-powered adversaries, we might gladly trade our liberty for protection; but can there be real protection in place of our ability to judge for ourselves?

Another dynamic adds to the urgency. Our migration to the Internet is following a *law of increasing intimacy*. As our devices cling more closely to us—smartphones, watches, laptops, voice boxes, and the next generation of gadgets – the stronger the superpowers grow. More proximate devices facilitate Interception, and the finer, more continuous stream of data they produce aids Intelligence. At the same time, the data improves the helpfulness of our devices and applications: think Fitbit, order-ahead Starbucks, and, in times of pandemic, contact tracing. The technology therefore improves with use, attracting more use—a self-reinforcing cycle that continually bolsters both the superpowers and our vulnerability. As our gadgets draw us in, they work incrementally to subordinate us to those who possess the superpowers.




This is the dilemma of the Internet Age: our intimacy with machines promotes progress and vulnerability at once. This Law of Increasing Intimacy with connected devices extends our Reach but erodes our agency. We've entered a Faustian bargain where we trade convenience for pieces of ourselves—for data, which fuels the seductive good but breeds dysfunction. Our response must be swift, far-reaching, and permanent.

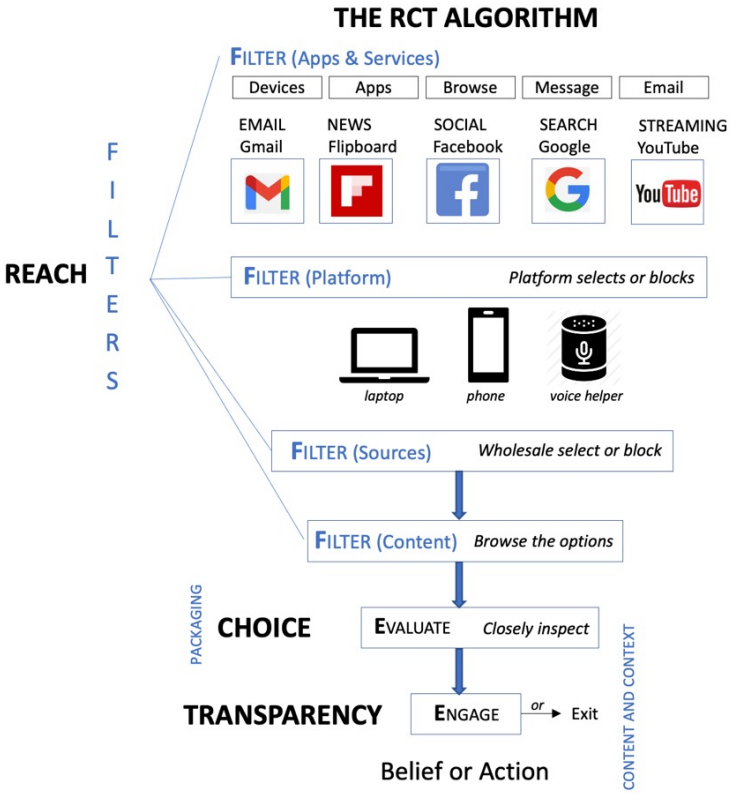
# Analysis

In thinking about civilizing our digital Wild West, it's helpful to consider how we bring order to our highway system. We regulate highways with a complex of signage, rules, and certifications to create a cognitive world where people can operate almost completely autonomously. Drivers have enormous latitude to make decisions but within well-understood rules. When we drive a car, we're free to choose our destination but not the side of the road to drive on or which color traffic signal to obey. Drivers are as free as they can be consistent with safety for all. And because the rules keep the streets safe when everyone follows them, we don't mind the constraint. Furthermore, we are happy to delegate the rule-setting to a public authority that leaves the rest of the decisions to us. The authority licenses drivers to certify they know the rules and can be found in case of mishap. With this accountability and a good set of rules, individuals need only modest supervision. And, in most places, the number of traffic tickets is small relative to the number of driving decisions. Highway regulation succeeds in promoting a very high degree of self-governance.

# A New Approach to Internet Regulation

The Internet is not only the highway but also the vehicle, terrain, and often starting point and destination – hence the need to consider the entire RCT. We increasingly manage our life experiences on the Internet from the top of our opportunity funnel down to the activities themselves. The diagram here illustrates how online life looks through the RCT lens.

The Internet provides applications, search engines, and various devices we use to set our Reach, our locus of alternatives from which we Choose. Because manipulating our upstream opportunities directly influences the choices available to us, the legitimacy of those higher-level Internet sources is vital to assuring free choice.




Once we make a choice, we need to be sure the elements of the engagement—new friend encounter, Peloton ride, political screed, or MASH rerun—are complete and genuine. Trusted transparency grounds our experiences.

However, shoring up our cyber RCT is not all we need. By the Law of Increasing Intimacy, the Superpowers will become a growing threat even to those with robust RCT equipment. Tactical remedies like those emerging around the world today will still be required. For example, the European Union and United States seek to restrict data collection (managing Intelligence) and targeted advertising (Interception); and Estonia, India, and China mandate persistent digital identities (preempting Invisibility).

Yet public authorities must take care not to bluntly dismantle the Superpowers. Restrictions must be skillfully crafted by knowledgeable people who understand how each power operates within a larger ecosystem. Banning data—Intelligence—would destroy valuable services. Interception is part and parcel of such conveniences as alerts, notifications, text messages, and phone calls. Even Invisibility plays an important role, as among whistleblowers or discreet social encounters, for example. Indiscriminately undoing the Superpowers risks throwing progress out with the peril.

# The Need for a Lasting Solution

While Congress attends to misinformation, surveillance ads, and data privacy, and the Department of Homeland Security, Department of Defense, and intelligence agencies guard our cybersecurity, Congress must work to guarantee self-governance on the Internet. Self-governance is good for personal liberty, but it's also the only practical way to manage billions of Internet interactions daily, which will only multiply with self-driving cars, robots, home 3D fabrication, conversational companions, and continuing waves of technological advancements.

While private enterprise keeps the wonders coming, regulators must keep tending to the Internet's vital infrastructure: the tools of safety and cooperation. Everyone needs secure cyber highways, the senses, skills, and signage to navigate them, and assurance that everyone else is similarly equipped. Online users need empowered autonomy because that is what we mean by freedom, and self-governance is the only model of cyber society that can work at scale.

The Internet needs a specialized federal agency to keep us safe, secure, and civilized through all the advancements of the next millennium. In the United States, we entrust our government with safeguarding our environment, air travel, highways, food, drugs, and stock market. Because it is increasingly home to all of these, the Internet might be the public's most precious charge. Yet it requires a brand-new regulatory approach. I propose some guidelines here.

# Recommendations

**Recommendation 1 (Permanent Agency):** Establish a cabinet-level government agency responsible for Internet governance. The agency's broad mission would be to assure citizens of cyberspace can seek desirable opportunities (Reach), with adequate information to choose among them (Choice), and clarity to experience what they choose faithfully (Transparency)—one might equate this to life, liberty, and the pursuit of happiness on the Internet.[1]

The new agency should have the specialized skills and broad legal mandate to develop policies that promote strong Internet self-governance while also attenuating incipient threats (e.g. election interference, data breaches, ransomware attacks) and chronic breakdowns (e.g. violent livestreams or misinformation adverse to public health). The new agency would have authority over Internet and artificial intelligence technology companies, data buyers (such as advertisers), and users, with a mission spanning safety, privacy, security, and education.

The agency will also forecast technological advances and shape policies to meet the Internet where it will be at least a decade in the future, both to anticipate imminent hazards (e.g. autonomous vehicle hijacking) and to equip users with smarter means of self-protection as technology evolves (especially natural language processing, large language models, and other kinds of artificial intelligence). With its primacy in understanding online behavior and future trends, the agency will work closely with cybersecurity operations and other organizations with Internet jurisdiction, such as the Federal Trade Commission and Federal Communications Commission, as well as agencies affected by trends in technology, especially Departments of Transportation, Energy, and Labor.

**Recommendation 2 (Senses):** The new agency should restore the faculties that equip people to protect their property and privacy, navigate safely, judge soundly, and trust each other. The agency would incentivize industry to apply emerging technologies to equip users with reliable "senses" (e.g. identification, video authentication, app labeling) and restore "natural laws" to the cyber environment (e.g. permanence, verifiability) prerequisite to confident *self*-governance within established rules.

a. **Enforce universal digital identification.**[2] Establish a tamper-proof, industry standard digital ID available to anyone to ensure that every interacting entity can have a known and certain identity. Display of one's ID is not required, though use of an alias is always declared. Various licenses and forms of identification will be required as the agency would administer appropriate certifications and licensing for data buyers, users, and app providers, possibly including device and app registration.

b. **Sanction labeling/rating critical resources**, such as Websites, applications, and publishers, just as the Food and Drug Administration mandates nutritional labeling of processed food. It could mandate methods for identifying the source of information transmitted, the algorithms used to deliver the information, and bias in the distribution of information, including search. It could also administer an emblem program for licensing major applications and machines to certify products are safe and operate as advertised. In the new digital world, one's safety record would be comparable to audited financial disclosures in public companies.

c. **Equip users with software tools** to identify suspicious uses, analogous to spam filters that analyze origin, classify meaning, and predict maker's motives with an eye to consumer protection. These tools would apply the latest AI techniques to assist with *deception detection*, tools that identify bots, fact check, and flag suspected fraud or even biased or exclusionary practices. One's personal chatbot – let's call it a personal agent – could assess hazards within one's sphere of activity and even learn to adjust for one's risk preferences.

d. **Incentivize secure and reliable reputational systems (a la Yelp, eBay, or Airbnb) and classification systems** to help people confidently filter and choose. This may include a *public registry* that crowd-sources reputational information where complaints and commendations can be reliably matched to users, data buyers, and providers.

e. **Support mainstays of trust**, such as academia, journalism, and public education to buttress both Choice and Transparency, the selection and comprehension of destinations. The agency would seek to support business models for digital press or general information (a la Wikipedia) repositories with subsidies and arms-length public assistance.

**Recommendation 3 (Superpowers):** As in the real world, the Internet requires both the cognitive framework for its users with the contours described above and a set of protections against incursions seeking to disrupt or manipulate self-governance. These are the critical steps for protecting against the Superpowers:

a. **Invisibility** will be mitigated by universal identification, while permitting anonymity and aliases so long as they are declared.

b. **Interception** (in email, apps, browsing, voice assistants, robot behaviors, and so on) will be reduced by mandating the use of the *digital ID* (and perhaps additional certification) by all data buyers, which should bring accountability and reputational transparency to anyone using data to target others. It can be further managed with *app credentials* and robust classification and filtering systems that allow users to fine-tune their environment to their taste, eventually employing a personal agent to assess and deflect. As the Internet becomes more immersive, opportunities for Interception will increase. Correspondingly, user controls must become more precise and easier to use. As natural language voice commands and physical gestures become the new mode of Internet navigation, Interception filters and adjustments for mood and shifting preferences must maintain similar levels of intelligence and ease of use.[3]

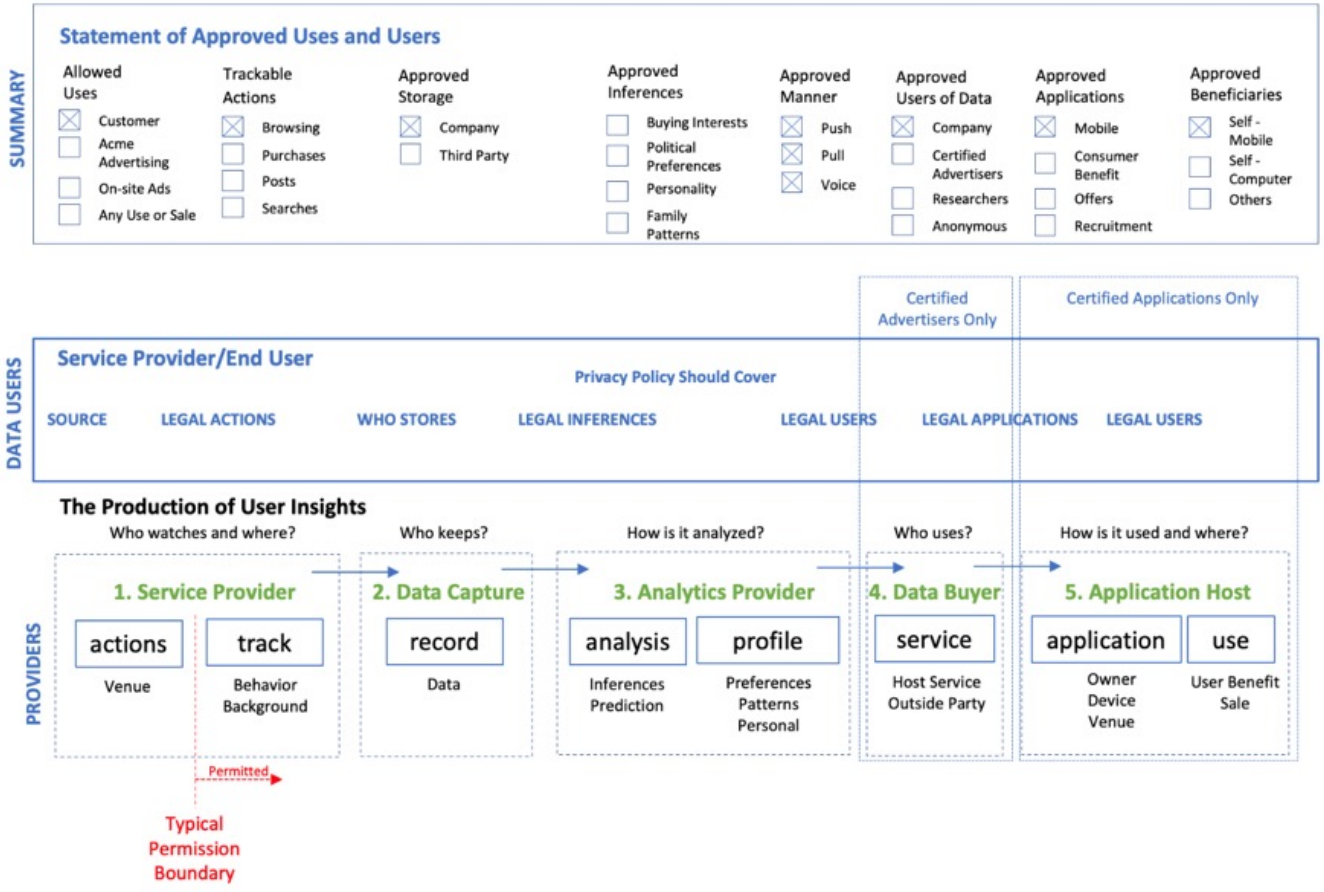
c. **Intelligence** can be managed with privacy controls and data sharing tiers emulating HIPAA guidelines and determining a data permission hierarchy that users can easily understand and control and that data buyers may use transparently (see next). A crucial goal will be to give users comparable Intelligence about data buyers as data buyers have about them. Advances for data buyers, including advertisers, should be matched, where possible, by similar capabilities for users.

**Recommendation 4 (Privacy):** Clarify ownership of data and establish a standard permission protocol allowing users to set permissions for any provider; set the rules by which different entities are permitted to touch data; and establish methods for partitioning data so that separate rules and controls for different categories of data could be supported. The new agency would source a dashboard for user monitoring of data collected, insights drawn, and uses by each provider with a privacy agreement – eventually (and hypothetically) managed and simplified by one's personal agent.

a. **Data use credentialing** of purchasers of data, equivalent to licensing parties wishing to use end-user data.

b. **Data use guidelines** helping to identify and manage the three types of data uses described earlier in this paper.

c. **Data permission and monitoring** tools for users, standardizing a vocabulary and language everyone can understand; a protocol for multi-level, multi-category data permissions; and a user-friendly dashboard for transparency and control.



**Recommendation 5 (Public Good):** Desirable public outcomes will not always result from individual behavior, no matter how well-informed and virtuous the individuals. Here is a sampling of areas where the new agency must watch for the common good:

**a. Content monitoring**. Given the opportunity to apply advances in NLP and AI to automate the task, private companies and public authorities must share responsibility for information moderation, which, for example, protects against:

- Mass manipulation of election-related information, including political ads, with particular attention to foreign purchases of social media;
- Misinformation adverse to public health;
- Illegal speech (e.g. real-time shootings, child pornography, threats against life or government).

Where blocking content is inappropriate, the public-private collaboration should improve spam-filter-like tools and personal agents that give individuals fine-tuned control in all venues, not just email.

**b. Cybersecurity**. It should be assumed that without persistent deterrent efforts, any system on the network will eventually be cracked. Sophisticated hacking nearly always begins with a ruse, which is the bailiwick of the new agency. It must work closely with the cybersecurity branch to devise network-wide protections against intrusion, theft, and sabotage.

**c. Public information**. The new agency would be responsible for conducting and promulgating research about (a) how the Internet and AI work (and don't work); (b) what data means; (c) moral hazard issues; (d) best practices guidelines; (e) forecasts of advancements and their impacts (on labor and transportation, for instance). *Fund and distribute research* into new advances, interfaces, classifiers, and protections, and supporting academic and industry research and development of the same.

**d. Public education**. Understanding the technology surrounding us should become a civic duty. Platforms and users must share a vocabulary so that when users are given control, they know what to do and what to ask for. Digital literacy should become an early education requirement.

**e. Data pooling**. Identify areas where compulsory inclusion of data may have social benefits (health, medical, DNA, contact tracing), anonymized where appropriate.

**f. Trust in technology providers**. Regulators must incent tech providers to take responsibility, perhaps making technology companies *information fiduciaries* legally responsible for protecting their users' safety and privacy.[4] With an enlightened outlook that sees public trust as necessary to their long-term viability, "safety" will become part

of their business model. However, *oversight should not overstep*. While establishing rules and deliverables for technology companies, regulators must respect the Internet's advancing value and the public's interest in this advancement. Successful regulation must balance protecting consumers with preserving sustained innovation and investment in tech companies.

**Recommendation 6 (International):** Since the Internet is a shared global resource without easily managed borders, the U.S. agency should model these principles and try to promulgate them to similar agencies worldwide, striving over the long term to establish a multi-national authority with streamlined standards and rules, charged with forecasting and planning for global advancing intelligence.

# Conclusion

Contending with COVID-19 has reaffirmed our network's indispensability. Aside from the Internet's other monumental benefits, our network builds social resilience, helping us to endure global calamities, whether war, pandemics, catastrophic climate events, or worse. Indeed, our massive and growing population likely needs the Internet for long-term survival. As with our climate, we cannot escape the Internet. We must make it civilized and habitable. And as our rough-hewn electronic frontier is rapidly enveloping us, the time to civilize it is now.

# About the Author

**Steve Johnson** was an early Internet inventor who patented the image compression algorithm that America Online used to create the first online pictures in 1993, paving the way for what is known now as streaming media. After AOL purchased Johnson-Grace company in 1996, Johnson ran R&D at AOL as it became America's front door to cyberspace in the early Internet age. Since leaving AOL in 1999, Steve has been a technology entrepreneur and investor, founding companies in video telephony, personalization, data extraction, handwriting recognition, and advertising technology. In 2018, he returned to the home of his graduate work, Harvard's Kennedy School, as a fellow at the Belfer Center.

# Endnotes

1 In February 2022, Congresswoman Lori Trahan and Senator Chuck Schumer proposed the Bureau of Digital Services and Safety, which is a first step toward the proposed agency. The Bureau, in its inception, would sit within the Federal Trade Commission.

2 In 2021, the U.S. House Financial Services Committee has established a Task Force on Artificial Intelligence, which is exploring the efficacy of secure digital identification that would "verify identity while preserving privacy in the digital age."

3 In January 2022, Congresswomen Anna Eschoo and Jan Schakowsky and Senator Cory Booker introduced the *Ban Surveillance Act* which aims to (dramatically) reduce the amount of data-driven Interception.

4 Balkin, Jack M., and Jonathan Zittrain, "A Grand Bargain to Make Tech Companies Trustworthy," *The Atlantic*, Oct. 3, 2016, and Jack M. Balkin "Information Fiduciaries and the First Amendment." *UC Davis Law Review*, vol. 49, no. 4, Apr. 2016..