HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

POLICY PAPER
belfercenter.org/homelandsecurity

HOMELAND SECURITY PROJECT | NOVEMBER 2022

Internet Superpowers*

Steve Johnson

Executive Summary

As inventions go, the Internet stacks up with the best of them: the lightbulb, automobile, maybe even fire. However, it's time for policymakers to look carefully at how its swift transformation of society has affected freedom. Today's disconcerting answer is that it breaks some essential tools for a civilized society. Furthermore, it equips people with "superpowers" that further rob individuals of their agency. Regulation focused on data privacy and misinformation misses this larger societal threat; public authorities must attend to civilizing the Web. The United States needs an agency devoted to empowering citizens to self-govern in cyberspace for generations to come. This call will reinforce U.S. strategic defenses against cyberattacks (for example, by the Cybersecurity & Infrastructure Security Agency (CISA) and the recent Cyberspace Solarium Commission). As this essay explains, bolstering the civility and transparency of our cyber lives also promises to reduce our vulnerability to such attacks.

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

Background

In 1992, when Sir Tim Berners-Lee blessed us with a new medium that 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. Not only a means of communication, it was also a brand-new mode of transport. Now, three decades on, it carries us to doctor's appointments, shopping malls, cinemas, and, most of all, to each other countless times a day. But Sir Tim failed to warn us of its secret curse: it ain't the world as we know it.

Our new home on the Web is like a cross between the wild west town of Deadwood and the fictional, fabricational world of the Metaverse, which, far from happening in the future, is unfolding around us now. We have been gradually moving there since Berners-Lee bestowed his magic markup language thirty years ago.

The little-recognized trouble is that 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. In this altered reality, the two cornerstones of self-governance—judgment and trust—break down. Self-governance entails the ability to manage our affairs and interactions with others with minimal supervision. Without it, freedom can collapse into chaos, or worse, captivity. The Internet may be putting self-governance to its toughest test ever.

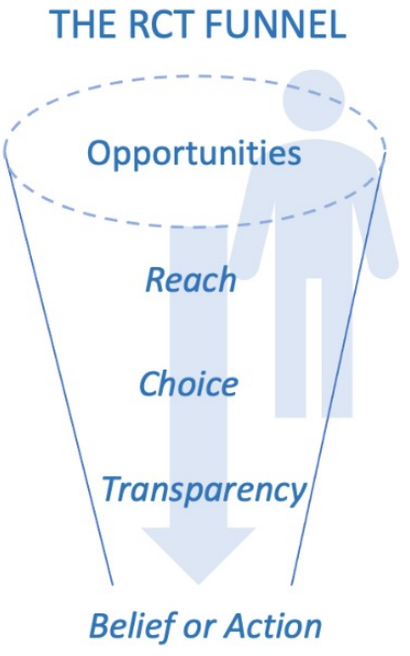
Measures to combat identity theft, invasive advertising, or ransomware miss a more serious challenge. Our vulnerability goes to the heart of what has enabled people to interact collegially throughout history: not only human qualities, such as reputation and identity, but physical facts, like solidity and authenticity. Responding to the concerns du jour is inadequate to this more profound regulatory need; it attends to bad cyber behavior without mending cyber society itself.

A "Conduct of Life" Framework for Internet Regulation

While addressing incipient issues and securing our network, regulators must also view the Internet through an anthropological lens to understand how to support people in governing their digital lives successfully. The goal is to equip cybercitizens to navigate and make decisions as well online as they can offline, yet without overwhelming the Internet with interventions. The Internet is not a medium like print or television where editorial adjustments can suffice; it is more like a city than a newspaper, where people need good senses and reliable information to live and cooperate effectively.

Consider the following 'conduct of life' model to guide the regulator in supporting self-governance on the Internet. It's based upon the notion that self-governance isn't only a matter of informed choice in the moment; it requires empowered freedom from the top of one's experiential funnel to the bottom. It rests upon three components that are required for personal liberty: reach, choice, and transparency.

The top of our life's journey is **Reach**, our wholesale cut, marking our perimeter and situating us in the world. It's our neighborhood, place of worship, news sources, family, and friends, defining what we encounter daily, ideally rich in what we desire and scarce in hazards and harm.



Choice is our reducing to those items or interactions we wish to consider more closely. We peruse the surface of things, including people, to estimate what's inside, choosing them based on their packaging, appearance, or name. Our success at this stage will depend upon how well we have curated our Reach and can judge things by their covers.

When we make a choice, **Transparency** is the clarity of the exchange. It supplements the content with the context behind the symbols, which are always just a shorthand. The transmission is never everything; the context is everything else. We incorporate available context and history into our experience and response, whether belief, action, emotion, or indifference.

Well-functioning Reach, Choice, and Transparency (RCT) is freedom in its fullest sense: liberty to access the world and the knowledge to comprehend it. *It is our algorithm of freedom.* Internet regulators must look both upstream and down this experiential funnel to see how the Internet affects where people sit (Reach), how they navigate their alternatives (Choice), and how they process what they choose (Transparency). Thus, the RCT offers the regulator a governance checklist for ensuring people can conduct their online lives satisfactorily.

Our RCT works well on terrestrial Earth because things are relatively stable and predictable, and we can perceive them directly. We can curate our world by watching, judging, and choosing. There is a symmetry between us and our counterparts whom we can observe and verify, and who can do the same. Reliable appearances facilitate our mind's simulation. When dealing with others, we know they can't easily disappear when things go wrong. The restauranteur and taxi driver serve us without advance payment because dashing and disguise are difficult and impractical. We carry our identities on our bodies, so we learn trustworthy behavior. Our reputation checks us. Honesty—or at least consistency—becomes second nature. Then old-fashioned loyalty and retribution, and institutions like laws and law enforcement fill the gaps that handshakes can't seal.

On the Internet, this civilized arrangement is scarcely detectable. Cyber objects and people aren't themselves but avatars—projections of reality. We know them not by sight or smell but by their labels. Cues to meaning and trustworthiness, such as context and track record, are suspect or missing. Identities are mutable, and so are their surroundings. We may see neither forest nor trees but fly (by hyperlink) to destinations without context. Speech on the Internet is often detached from origin and author, information critical to the listener's comprehension. The packaging and essence of what we interact with on the Internet are fluid, leaving anchors of civility and trust without ground. Our adolescent Internet offers only thin ethical and legal reinforcement. By 21st-century standards, it is still barbaric.

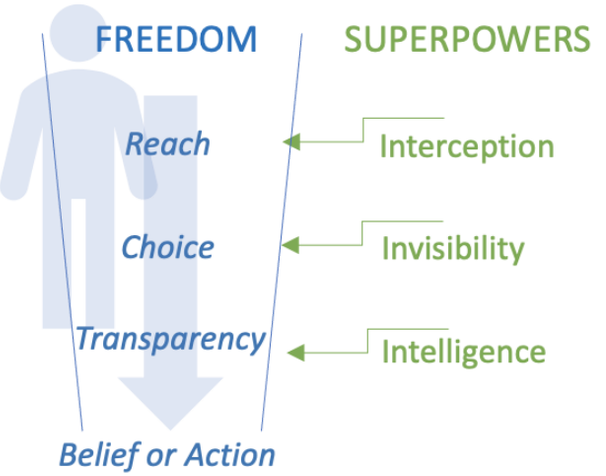
Because most prior forms of community were close and tangible, we assume it will function just as well electronically. So, we keep migrating online, coveting the openness we construe as freedom even while sensing a growing danger. Regulators scramble to patch the Internet's defects with data restrictions to allay privacy concerns and content moderators work to remove harmful fakery. But breaches of privacy and responsibility are only markers of a place where certainty and accountability are too scarce for comfort.

The Internet's Superpowers

The danger arises because we have invented an alien environment that lacks the prerequisites for self-governance that human societies have always possessed. The Internet shrinks our acumen for bracketing the world, assessment, decision-making, and experiencing what we choose—it debilitates our RCT. It provides porous perimeters, misleading signage, fabricated facades, and transitory people and things. It equips us with only the crudest of sensory tools. It lacks coherent laws, patrol cars, or 911. But, most frighteningly, it confronts us with concerted forces—powers harnessed by others—that can thwart the functioning of our RCT.

Imagine the disruption to self-governance if comic book superpowers such as teleportation, shapeshifting, and mind-reading existed in the real world. Well, these superpowers of fables and fairy tales have already arrived in the form of the insidious forces of the Internet. Anyone with a credit card can harness the Internet's platforms (Google, Facebook, Apple, and others) to intercept other users at any moment, 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.

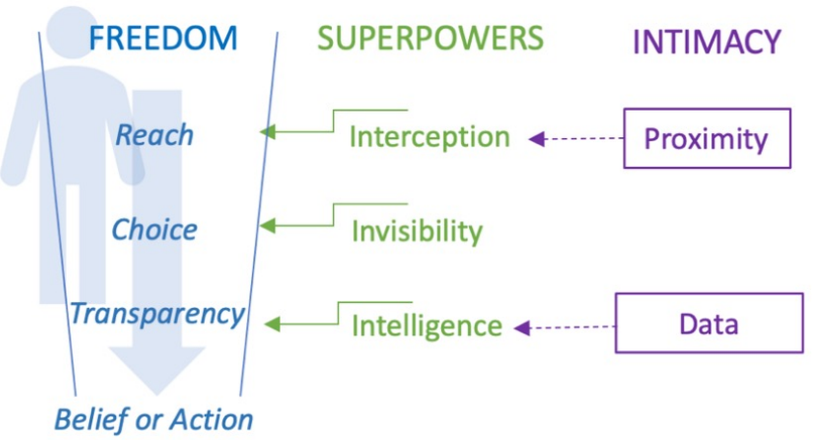


Invisibility, like shapeshifting, is the ability to change identities at will—threatening Choice. The Internet provides unlimited aliases (account names, email addresses, dating handles, and so on) at little cost, with no means of verifying aliases, linking them across applications, or guaranteeing they 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 computerized capabilities. When strangers can freely enter our space, shift to any identity, or know us better than we know ourselves, our online lives become a dream where trust in people or 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 follows a *Law of Increasing Intimacy*. The more personal our devices—smartphones, watches, laptops, voice boxes, and superior gadgets of the future—the stronger the superpowers. Proximity aids Interception, and more sensitive data aids Intelligence. At the same time, our applications become more helpful: think Fitbit, order-ahead Starbucks, and, in times of pandemic, contact tracing. Technology improves with use, which in turn attracts more use—a self-reinforcing cycle that continually adds to the superpowers and our vulnerability to them. While our gadgets become ever more attractive, they will, unbridled, guarantee our subordination to those who possess these capabilities.



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 machines extends our Reach but creates divisive powers antithetical to our ability to self-govern. It is a Faustian bargain that is slowly eroding society. Our response must be swift, far-reaching, and long-lasting.

Analysis

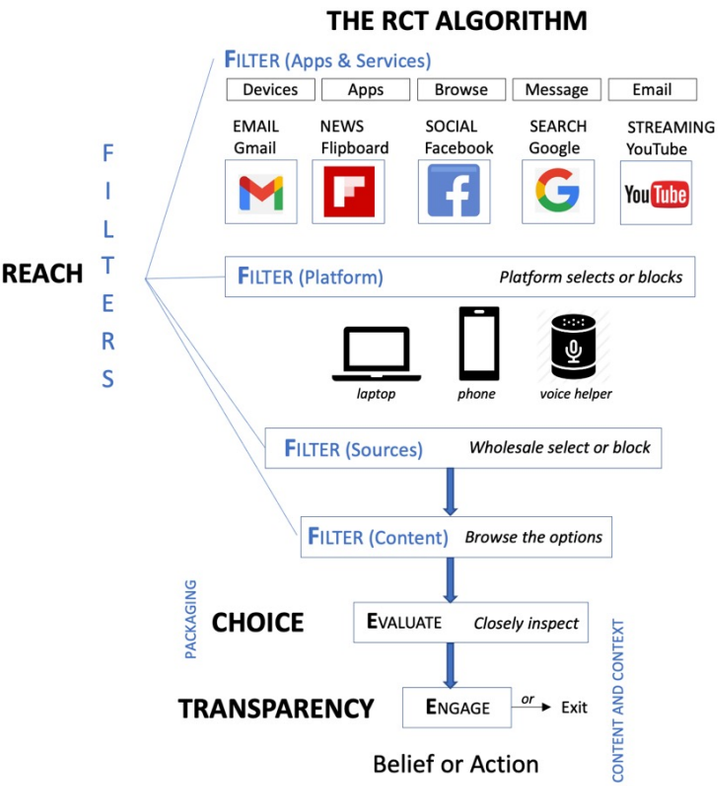
Comparing the Internet to a highway system provides some useful insights. We regulate highways with a constellation of signage, rules, and certifications to create a cognitive world where people can operate almost wholly autonomously. Drivers have enormous latitude to make decisions but within well-understood rules. When we drive a car, we're free to choose our destination but not the side of the road 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 Oversight

The Internet is not only the highway but also the vehicle, terrain, and often starting point and destination. This is why any regulatory authority needs a "conduct of life" model like the RCT. We increasingly manage our life experiences on the Internet from the top of our opportunity funnel down to the activities themselves. Here's how online behavior looks through the RCT lens.

The Internet provides us with applications, search engines, and various devices we use to set our Reach, our locus of alternatives from which we Choose. Because manipulation of our upstream opportunities could mean that any given choice is not as free as it might seem, the legitimacy of those higher-level Internet sources is vital to assuring free choice.

Once we make a choice, then we need to be sure the elements of the engagement—whether a new friend encounter, a Peloton ride, a political screed, or MASH rerun—are complete and genuine. No experience stands completely alone; context is always needed for a full understanding. Therefore, assured (or nearly assured) Transparency is needed to ground our experiences.



However, shoring up our cyber RCT is not all we need. By the Law of Increasing Intimacy, the Superpowers will become an increasing threat even to those with robust RCT equipment. Tactical remedies will still be required.

Regulators worldwide currently tackle the Superpowers head-on. The European Union, United States, and others seek to restrict data collection (Intelligence) and targeted advertising (Interception). Estonia—and China, for that matter—mandate persistent identity (preempting Invisibility). But regulation must not dismantle the Superpowers altogether. Restrictions must be crafted carefully by skilled, knowledgeable people who understand how they operate 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. Indiscriminately undoing the Superpowers will discard progress along 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 toward strengthening 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 autonomous vehicles, robots, home 3D fabrication, conversational voice recognition, and other technological advancements.

While private enterprise keeps the wonders coming, regulators must keep attending to its vital infrastructure: the tools of social cooperation. Each individual needs safe cyber highways, the senses and skills 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 important charge. Yet it requires a wholly different regulatory approach. Here is an outline of guidelines.

Recommendations

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

The new agency should have the specialized skills and broad legal mandate to develop policies promoting 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 regulate Internet and Artificial Intelligence (AI) technology companies, data buyers, and users, recognizing that some affected entities, such as advertisers, are not technology companies. Its rules will span 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 hence, 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 (NLP) and other kinds of artificial intelligence). With its primacy in understanding online behavior and future trends, it will work closely with cybersecurity operations and other agencies with Internet jurisdiction, such as the Federal Trade Commission and Federal Communications Commission, as well as agencies affected by trends in technology, especially transportation and labor.

Recommendation 2 (Senses): The new agency should restore the faculties that equip people to trust each other, navigate accurately, and judge soundly. The agency shall collaborate with industry to equip users with reliable "senses" (e.g. identification, video authentication, app labeling) and restore to the cyber environment critical "natural laws" (e.g. permanence, verifiability) needed to allow users to confidently *self-govern* 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 also 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 (e.g. robots) 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 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.

d. **Incentivize secure 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 that would seek 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* by all data buyers, which should bring accountability and reputational transparency to anyone targeting 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. As the Internet becomes more immersive, opportunities for Interception will increase. User controls must become, correspondingly, 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 precision and ease of use.[3]

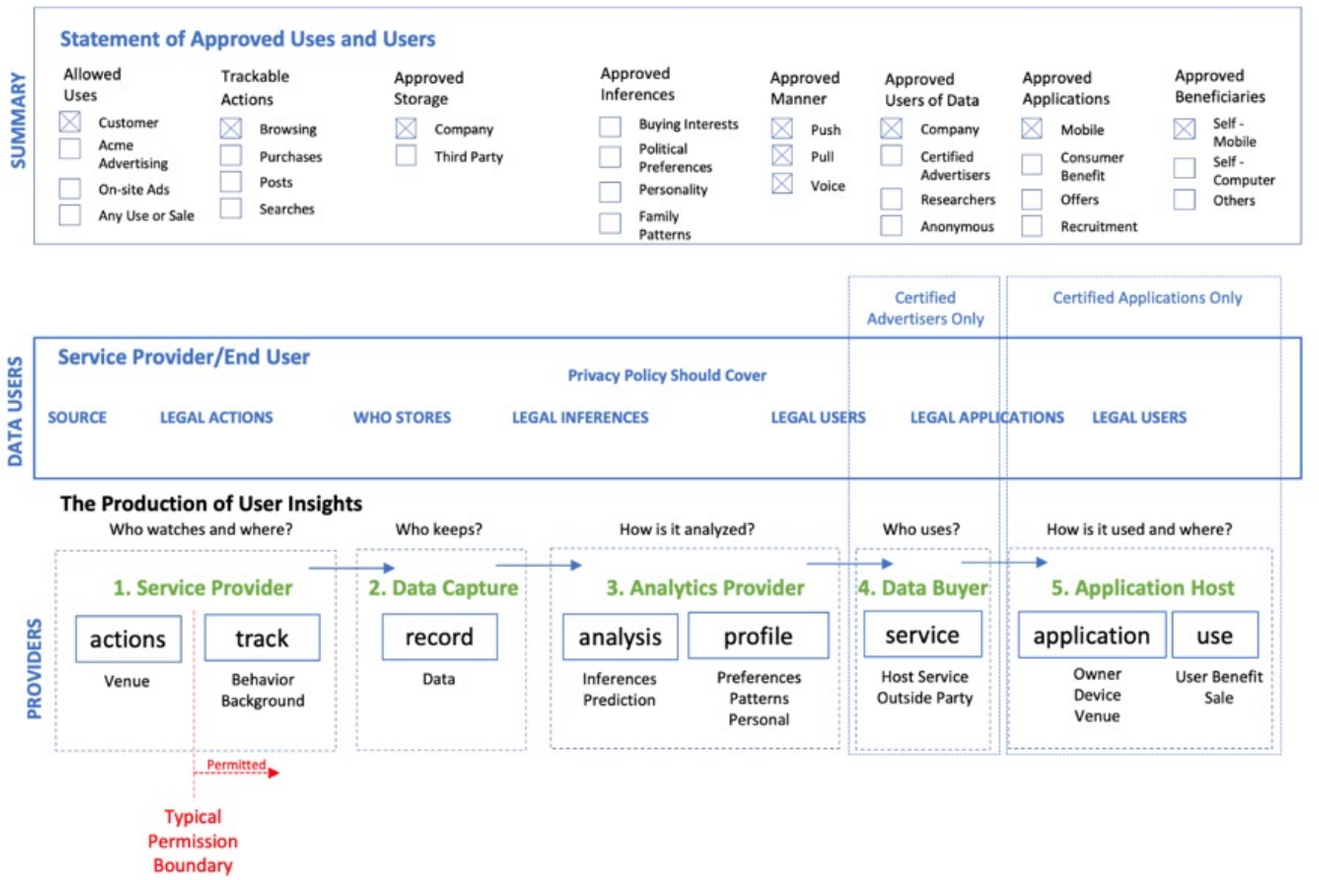
c. **Intelligence** can be managed with privacy controls and sharing tiers emulating HIPAA guidelines and determining a data permission hierarchy that users can easily understand and control and that data buyers may use transparently (see next). A crucial goal will be to give users comparable Intelligence 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 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 whom they have a privacy agreement.

a. **Data use credentialing** of purchasers of data, tantamount 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 even well-informed, virtuous individuals. Here is a sampling of areas where the new agency must watch out 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 will share responsibility for information moderation, which, at a minimum, 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 that give individuals fine-tuned control in all venues, not just email.

b. Cybersecurity. It should be assumed that without continuous deterrence 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; (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. Educate the public. Understanding the technology surrounding us should become all citizens' 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. Online literacy could become a Digital ID requirement.

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

f. Trust in technology providers. Regulators must incent tech providers to take responsibility, perhaps making technology companies *information fiduciaries* who are

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 promulgate these principles and serve as a model to similar agencies worldwide. A multi-national authority might be considered, charged with forecasting and planning for global advancing intelligence.

Conclusion

Contending with COVID-19 has reaffirmed that our networked machines are nearly indispensable. Aside from its other monumental benefits, our network builds social resilience, helping us 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. But we must make it habitable—and civilized.

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 2020, 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.