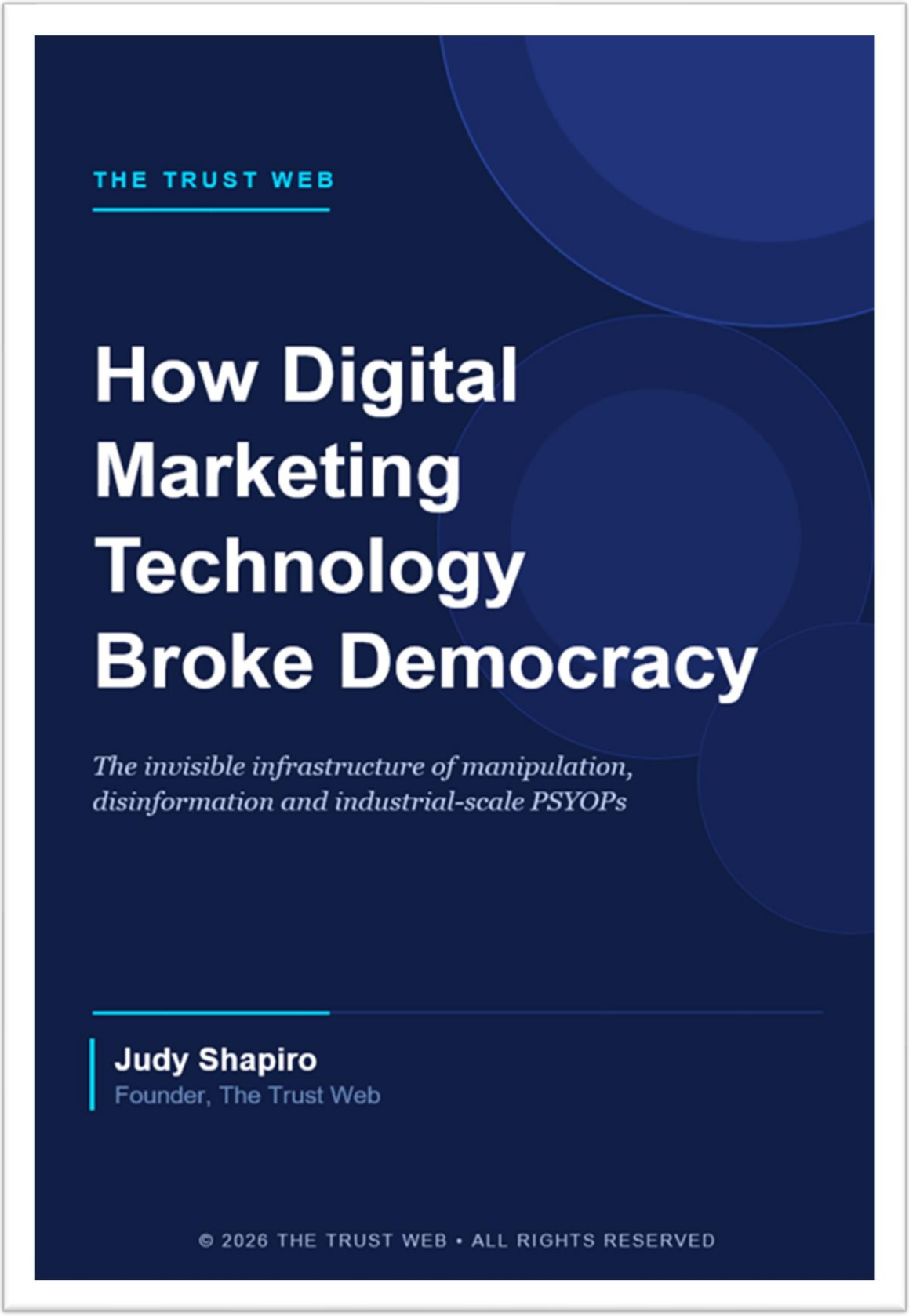


EXECUTIVE SUMMARY

How Digital Marketing Technology Broke Democracy

The invisible infrastructure of manipulation, disinformation, and industrial-scale PSYOPs

A white paper by Judy Shapiro, Founder, The Trust Web

I. Introduction

Since roughly 2010, digital marketing technology (martech/adtech) has become the dominant way brands reach audiences. In fifteen years, the infrastructure built to sell soap, software, and cars has been repurposed into the most effective psychological-operations apparatus in modern history.

The fall-out is stark. V-Dem now reports there are more autocracies (91) than democracies (88) — a first in over two decades. Half the world's remaining democracies are in decline. In the U.S., 64% of adults believe democracy is "in crisis and at risk of failing," and trust has collapsed across the legal system, elections, science, healthcare, and government.

These outcomes trace to a specific, nameable infrastructure — roughly 15,000 digital marketing technology companies whose business model was engineered for frictionless distribution of advertising to mass, 'scale' audiences. Autocrats and bad-faith actors discovered that the same plumbing that delivers lots of ads to lots of people, delivers disinformation just as efficiently.

II. The Villain and the 'Unknowable Distortion Field'

Naming the Culprit

The villain hiding in plain sight is the digital marketing and advertising ecosystem — ad networks, social platforms, programmatic exchanges, profile-data brokers, and their algorithms. In the race to serve advertisers at scale, this ecosystem adopted trust-busting practices as a feature, not a bug. Verification was engineered out because it reduces inventory, and reduced inventory reduces revenue.

Four technical pillars in digital marketing made the damage possible: cheap, easy-to-use messaging distribution; scale algorithms that reward repetition and build echo chambers; engagement-optimized ranking that amplifies outrage; and the near-total absence of verification. Built for advertisers, these pillars were well leveraged by propaganda operations worldwide.

The 'Unknowable Distortion Field'

The global harm caused by digital marketing technology can remediated if we are precise in understanding this apparatus which we can refer to as the 'Unknowable Distortion Field.' This is a

psychological space that occurs when virtually nothing can be verified online. Mistrust becomes pervasive in the very foundations of healthy cultural functioning; institutions, science, elections, experts, and even the motives of everyday online strangers as all become suspect.

The 'Unknowable Distortion Field' is not a new phenomenon which is noteworthy because past experiences with the 'Unknowable Distortion Field' is instructive for how to deal with it today. The last time humanity confronted this level of mass confusion of thinking was during the Dark Ages - from 500 to 1100 CE. Caused by the Roman Empire's collapse, this event produced an information void which was terrifying to people. In the absence of "knowable" information, people put trust in "unknowable" forces such as alchemy, astrology, and black magic; forces that felt redemptive but offered little real-world protections to vulnerable populations.

This epoch teaches us something important for our current situation. Today's dynamic, belief in the unknown versus facts, is the mirror image to what people experienced 1,000 years ago but with a twist: people living in the Dark Ages suffered from too little information whereas today we suffer from too much **untrusted** information. Both states produce the same outcome — the public's preferences for beliefs that are unverifiable and a willingness to put primacy on "unknown" forces instead of facts. Similarly, both eras trigger the same cultural shift: from self-reliance and agency in navigating a difficult world to dependence on external entities for protection and guidance.

The 'Unknowable Distortion Field' broke the soul of democracy because democratic functioning depends on good-faith conversations about shared facts. When trust is disposable, this weaponizes content and their messengers so elections can be declared fake without evidence and political atrocities can be obscured by armies of troll accounts.

A knock-on effect of the 'Unknowable Distortion Field' is that key constitutional rights such as the First Amendment — meant to protect citizens who criticize power — becomes collateral damage in the capitulation of truth to flagrant bad actors leveraging armies of propogandists.

III. The Trust Web Is the Solution

The answer is not to dismantle digital marketing tech but to rebuild it as the Trust Web: a verifiable, privacy-preserving, user-controlled trust layer in which AI becomes a trust force rather than a manipulation force. The transformation requires coordinated action from three stakeholder groups.

Advertisers (and Their Agencies)

Advertisers hold the ecosystem's purse strings, making them the single most powerful lever for change. They must:

- Assume digital inventory is faked or fraudulent until proven otherwise, and pressure vendors and verification firms accordingly.

- Redirect budget toward trust-cultivating outlets — local news, radio — even where this means higher labor costs.
- Demand full transparency on where ads run, so dollars stop subsidizing hate content and made-for-advertising sites.
- Migrate from third-party tracking to first-party data, and push agencies toward topic-based targeting and direct buys with quality publishers rather than programmatic scale.

Technologists

Because technology dissolved civic trust, technologists bear unique responsibility to rebuild it. The work splits across three layers:

Marketing-tech trust tools — AI-driven Topic Intelligence that tracks topics rather than people; Trust Agents that communicate user intent without exposing identity; and blockchain-verified ad supply chains that close the fake-impression loophole.

Personal Trust Tech — Personal AI Trust Agents (PAITAs) as a private buffer between user and web; Decentralized Identity and Zero-Knowledge Proofs replacing "Login with Google" with user-owned identity wallets; and federated learning so personalization happens on-device.

Browser-activated trust — a "Trust Cockpit" replacing all-or-nothing privacy with granular, per-persona controls; sandboxes sharing "interest tokens" instead of identities; and C2PA content provenance labels exposing how content was made and whether it has been altered.

Politicians

Politicians have been convinced regulation is impossible in this space. However, this is a missed opportunity because politicians can be a huge part of the solution. The place to start is with social media firms because they are the super spreaders of disinformation. They evade oversight because they occupy the unmonitored Reuleaux Triangle where communications, media, and advertising overlap, yet with none of the obligations of any.

The remedy is one that politicians already know how to execute: taxation. Modeled on the Universal Service Tax telecom carriers now pay, this type of tax would require platforms to pay a tax on every active account. The upside is significant in that it would force these platforms to purge fake accounts since each fake account would now cost money plus it can also dismantle the scale-monetization formula. This approach requires no bespoke regulation so it can plausibly pass on a bipartisan basis.

IV. Why the Trust Web Is the Path Forward

The Trust Web works because it aligns with, rather than fights, the content-serving DNA of the Internet. It does not ask anyone to give up the benefits of personalization at the expense of privacy.

It does not require users to constantly look over their digital shoulders for dangers lurking in the dark at the expense of normal exploration on the open web.

It asks the ecosystem to build verifiable trust foundations — provenance for content, verified identity for accounts, user-controlled data for individuals, and topic-based rather than person-based targeting.

No single law, company, or piece of software can restore trust alone. It requires a coordinated realignment: advertisers redirecting demand, technologists building the trust layer, politicians closing the Reuleaux loophole, and consumers refusing to outsource their thinking.

The payoff is a digital renaissance that ends the modern Dark Ages. The Trust Web is a web where users have agency, content carries its origination story, AI is a trust force, and democracy again rests on the shared facts it requires. The 'Unknowable Distortion Field' can be dismantled because it is the predictable output of specific technical and business choices. If we make different choices, the current untrusted web can be reengineered to put trust at the center of our online experiences.

Trust in that.

How Digital Marketing Technology Broke Democracy

Since its mainstream adoption around 2010, digital marketing technology—commonly known as martech or adtech—has become the primary way brands reach their audiences. Over this relatively short period, these marketing platforms have created massive communications capabilities producing unintended but grim consequences that has put our democracy at serious risk.

To say that these technologies have actively unraveled the democratic fabric of nations worldwide is not hyperbole but an accurate reflection of facts on the ground. This paper will lay out how the mechanisms of digital marketing tech, originally designed for marketers to reach audiences "at scale," have been hijacked by autocrats and despots into an incredibly effective psyop apparatus that has put democratic governments in decline worldwide.

Democracy on the Decline – A Global Phenomenon.

It is noteworthy and alarming that V-Dem Institute's most recent report found, for the first time in over 20 years, the number of autocracies (91 countries) now exceeds the number of democracies (88 countries), a finding that underscores the global democratic decline over the few last decades, (Source: https://www.v-dem.net/documents/60/V-dem-dr__2025_lowres.pdf).

Additionally, Reuters reports: "Half of the world's democracies are in a state of decline amid worsening civil liberties and rule of law while already authoritarian governments are becoming more oppressive... [with] issues ranging from restrictions on freedom of expression to increasing distrust in the legitimacy of elections," (Source: https://www.reuters.com/world/half-worlds-democracies-decline-intergovernmental-watchdog-2022-11-30/).

Zooming in on the U.S., we see decline play out as of this writing (2026). According to an NPR poll; **"64% of Americans believe U.S. democracy is 'in crisis' and at risk of failing."**

It is not, therefore, an exaggeration to say that democracy has been brought to its knees. The real culprits, though, often go unnamed. We settle for simplistic answers blaming the press and social media, or more sinisterly, "unknown" vague villains such as secret cabals.

No matter who the finger of blame is pointing at, by missing the real offender, we are left powerless to combat the underlying culprit hiding in plain sight. Without clearly understanding the "who," we are unable to develop meaningful "how" responses that could work in the real world.

The Culprit Hiding in Plain Sight.

Let's be clear then.

The villain in this story is the digital marketing and advertising ecosystem, often referred to in general terms as digital marketing tech. Taken together, all these technologies form a massive infrastructure that enables marketers to reach global audiences at unprecedented scale, allowing their messages to spread further and faster than ever before.

The heart of the matter is that in the race to serve advertisers, digital marketing tech adopted trust-busting practices and protocols that had profound albeit unintended consequences in the larger public domain.

At the most fundamental level, digital marketing tech dissolved the trust glue that binds countries, communities, and culture by causing everyone to doubt everything they think they know.

Nothing can be verified so everything is suspect and untrustworthy; institutions, science, governments, politicians, business leaders and most often people we interact with online. Trust "signals" that dominated the real world have been drained away in digital experiences by the profit machinery of marketing tech.

To effectively combat this damaging dynamic, we need to understand it well. We do that by assigning a name to the damage caused by digital marketing tech: The 'Unknowable Distortion Field', (https://trustwebtimes.com/the-unknowable-distortion-field-is-eating-the-world-2/). As we will see, the effect of this phenomenon reaches deep in our collective psyche to cause us to look at everyone and everything with suspicion.

The Mechanisms of the 'Unknowable Distortion Field.'

The "Unknowable Distortion Field" thrives in the void between the diminishing realm of what is trusted and known, and the increasing domain of what is unknown, untrusted, and feared.

The DNA of the "Unknowable Distortion Field" lies in the business model of digital marketing tech — a model that trades in the unreal digital world, selling impressions that can be fake, clicks that are faked, and content outlets designed to generate ad dollars, devoid of any journalistic value or integrity. In its pursuit of frictionless ad distribution and maximum revenue flow, this technology eschewed verification altogether, deliberately dismantling the trust guardrails that defined communication protocols of previous eras. The result was a "trust loophole" baked into the very plumbing of digital marketing technology systems and infrastructure.

It is no surprise, then, that this technology "escaped" the marketing world to become the tech muscle for anyone with an agenda and enough determination to exploit digital ad platforms to distribute content relentlessly. Bad faith actors walked straight through the trust loophole, counting on the fact that people had no tools to cope with the tsunami of objectively false and fabricated information now flooding our digital public square at unprecedented "scale."

This is why conspiracy theories arise — pizza joints becoming sex trafficking hubs — and why personal attacks become so fierce for just voicing an opinion. The "Unknowable Distortion Field" creates the opening for unscrupulous charlatans and despots to step in and override the logic or experience of the individual. People stop trusting themselves to "know" anything, so they just look to know how their opinion leader thinks to be able to "know" what is "true."

As a tragic result, few constraints were placed on bad actors' ability to manipulate people into the 'Unknowable Distortion Field,' where people believe they cannot 'know' or trust anything. In the fallout, everyone was affected in deeply disturbing ways:

- General consumer mistrust in the rule of law: Pew reports that 62% of U.S. adults say the U.S. legal system is "not fair" to most people, (2024).

- Deep generational mistrust in key political institutions: It is now common for people to distrust election outcomes, especially among younger demographics where 46% of all voters under 35, report "not much" or "no confidence at all" in the integrity of election outcomes, (NBC News/Wall Street Journal).
- Eroding trust in science and research: 27% of U.S. adults now say they have "not too much" or "no confidence" in scientists to act in the best interests of the public. This is up from roughly 12% in 2019, (Pew 2024).
- Collapse of trust in healthcare systems: Gallup has found that approximately 66% of consumers report having "some," "little," or "no" confidence in our healthcare systems. Specifically, 31% fall into the "very low" or "none" category, (2024).
- Cynical mistrust in politicians to do right by the country: Only 22% of Americans say they trust the government in Washington to do what is right "just about always" or "most of the time." This leaves 78% of voters who express "low" or "no" trust.

Among all these statistics, the final one stands out as a five-alarm warning of the crisis on our doorstep. For democracies to function, we need good faith conversations – discussing policy options, the collective future, and plans for achieving social justice. Yet digital marketing tech demonstrated that trust and truth were disposable in the mechanisms that power the broad distribution of content. Digital marketing tech allowed bad actors to succeed on par with advertisers to reach massive audiences – at “scale.”

The direct fallout is that digital marketing tech caused a systemic shift; a reshaping the world’s collective perceptions to favor the “unknown” instead what is “known” with devastating consequences:

- Digital marketing tech weaponized content itself (all kinds) that traumatizes all of us.
- Digital marketing tech prioritized outrage content for the widest distribution because it was highly monetizable. This is exactly the type of content that radicalizes young minds.
- Digital marketing tech made political polarization, not new in American history, operate at scale.
- Digital marketing tech made trust disposable, which then revealed the full fragility of democracies that rely on facts to be broadly trusted.
- Digital marketing tech allowed everyone to be a publisher – even those voices whose content should not be so easily distributed. Nothing could be verified as true. The loudest voices were winning – true or not.

This overwhelming amount of untrustworthy content and “people” in the digital public square, eroded trust in everything, making everything “unknowable.” It became increasingly clear that with the right content engine in place, elections can be declared fake without hard evidence and countries can whitewash the worst of crimes with just a few thousand paid troll accounts churning out content that is deliberately distorting the truth.

Content became digital bullets assaulting us all – all the time - delivered by* untrustworthy "profiles." *This is the 'Unknowable Distortion Field' in action. By giving it a name, we can begin to formulate remedies.

THE PAST TEACHES US ABOUT THE REMEDIES FOR THE FUTURE.

To be more informed about how to combat the 'Unknowable Distortion Field' today, history provides valuable context to understand the current situation. It is not an exaggeration to say we are living a modern version of the Dark Ages where, 1,000 years ago, the 'Unknowable Distortion Field' was a phenomenon that dominated everyday lives for a long, long time.

It was during this period that humankind experienced a deep confusion of thinking which gave rise to the aptly named Dark Ages. From 500 AD to about 1100 AD, when the Roman Empire collapsed, this era was characterized by a dramatic information void caused when learning, math, and scientific exploration went silent in the chaotic and violent aftermath of the power gap. During those 600 years, people relied more and more on "dark" belief systems around "unknowable" magical forces: alchemy, astrology, numerology, and of course black magic to make sense of their changing world. They were desperate for anything that could help them deal with the many challenges they encountered in life – even if these methods seem outlandish to us now.

This was the appeal of the 'Unknowable Distortion Field:' it felt redemptive, providing a comforting but ultimately a false sense of security.

As populations became more and more insecure in the upheaval, soon enough, people became trapped in the 'Unknowable Distortion Field' not knowing which unknowable forces to trust. No wonder we find the dominance of superstitious beliefs and sectarian violence throughout the Dark Ages.

The influence of the "Unknowable Distortion Field" ran so deep during those centuries that the process of escaping it took many centuries. It started slowly with the Renaissance in 1300 CE through the Age of Reason in the 1600s impacting the upper classes first. It took another three centuries for the grip of the "Unknowable Distortion Field" to loosen enough for most people to break free.

HOW THE 'UNKNOWABLE DISTORTION FIELD' APPLIES TO US TODAY.

The parallels to today are startling because the Dark Ages and our contemporary moment share a strikingly similar dynamic; the public's preferences for beliefs that are unverifiable and a willingness to put primacy on "unknown" forces instead of facts.

In the Dark Ages, unknowable forces may have been unverifiable but they provided an information-starved population with a "safety net." Our modern crisis is driven by the exact same dynamic but with a twist. Instead of having too little information, we face an overwhelming flood of untrusted information that makes the truth impossible to discern. We then are easy prey to cults and hate groups who position themselves as a modern version of a "safety net."

In both epochs, populations are overwhelmed by transition and turmoil so that people's confidence in what we think we know begins to erode – allowing many to quietly slip into the

‘Unknowable Distortion Field.’ As people enter the ‘Unknowable Distortion Field,’ they lose agency: abdicating their power to anyone who can tell them what to think, what to “know” and what is “true.”

The damage of the ‘Unknowable Distortion Field’ is so acute because people reject the real world in favor of participating in the mass “unknowing.” Their whole identity is now tied to maintaining the wickedness of “unknown villains” or “dark forces” to signal their loyalty to the group.

In this state of 'unknowing,' they clutch more fiercely to the group's belief systems to remain 'safe' within the group dynamics.

This sets the stage for influencers with huge platforms to say, “I am just asking questions” with a highly biased insinuation knowing that their hidden message is amply communicated without context or facts. Virtue signaling emerged as a by-product of the ‘Unknowable Distortion Field’ because digital tech powered everyone’s ability to broadcast their adherence to group think that, in turn, became their “identity” signaling.

The underlying dynamic pattern persists over the millennium; people abdicate their personal agency in favor of powerful, external entities for protection in times of “unknowing.” This is the opening that bad actors exploited – all powered by digital marketing technology.

The Knock-on Effect: Constitutional Battles Playing Out Due to Digital Marketing Tech.

Amidst the serious consequences of the ‘Unknowable Distortion Field,’ we see important constitutional rights under relentless assault as well.

For example, the First Amendment to the U.S. Constitution, considered a cornerstone of American democracy, which protects freedom of speech, religion, the press, assembly, and the right to petition the government for a redress of grievances, is being undermined every day.

In 1791 when the First Amendment was adopted, freedom of speech was broadly understood in the context of guaranteeing people the right to comment, criticize and question the government and politicians without fear of retribution.

Over the course of our history, the First Amendment has been both expanded to include broader definitions of free speech, but it also has been limited about what is not protected such as the proverbial yelling “Fire” in a crowded theater which is a prosecutable crime. All these nuances are lost in the brute muscle of digital marketing tech.

Today, the rights guaranteed under the First Amendment have been distorted to protect actions our forefathers never imagined. Today, digital marketing tech provides cover to protect the most flagrant bad actors or “pundits,” who twist truths to serve their monetization or political Interests. They are free to have their platform to say what they want but they are not free from consequences of their content.

All this harm was made worse by marketing tech algorithms which did the heavy lifting that trapped people in the ‘Unknowable Distortion Field’ through the echo chamber effect. While this helped digital marketing firms make more money, (all content - good and bad - was monetizable), the damage, we all can see, runs deep.

Without the ability to contextualize the truth of any content or people distributing content, the foundations of democracy's long-standing dependence on shared truths and shared stories among its citizens began to crumble — slowly at first but at an accelerated rate that is alarming.

REVERSING THE DAMAGE OF THE 'UNKNOWABLE DISTORTION FIELD.'

To step back from the ledge, we must be precise in understanding the mechanisms of digital marketing tech that is the power plant of the 'Unknowable Distortion Field.' In terms of impact, digital marketing tech punches far above its weight class, given there are only about 15,000 companies in this segment, including a range of firms such as ad networks, social media like Facebook and Google, as well as a huge segment around publishers and profile data management.

As a result, this rather niche category makes itself felt far in excess of its business footprint by creating a perfect platform for menacing actors to breakdown democracy through unfettered access to unlimited audience access, broad distribution capability with virtually no constraints.

The business model of digital marketing tech rests on four tech pillars which enabled it to inflict so much damage with remarkable efficiency:

1. Content Distribution Platforms That Are Cheap and Easy to Use. Digital marketing tech puts incredibly powerful broadcast tools in the hands of anyone with a keyboard. The tech part of digital marketing tech made using these platforms very easy to use so everyone, literally, **had a highly efficient platform to broadcast anything and everything**, often for free or at very low cost. In a short amount of time, digital marketing tech weaponized all forms of mass communications well beyond digital marketing's need to run soap ads.

2. Content Distribution Capabilities at "Scale." The money-making machinery of digital marketing tech was its scale platforms and algorithms. These technologies were designed to push content and ads as fast and as broadly as possible. **This distribution capability turned out to be very useful for any well-oiled propaganda machine.** A key element of scale reach is the ability to repeat the same message over and over again until lies are transformed into faux truths.

3. Outrage Content to Game the Digital Tech Platforms: One of the less obvious pillars of digital marketing lies in its ability to get engagement from audiences. Advertisers cherish engagement as a way to get "intent signals" from prospective customers. Digital tech algorithmically rewards advertisers who create campaigns that get good engagement by showing it to more people so the advertiser will run the campaign longer. This became a new monetization opportunity for digital tech since successful campaigns that drive conversions incentivize advertisers to run more ads.

This algorithmic mechanism, alas, works just as well for bad actors. **Outrage posts get great engagement and digital tech platforms reward this type of content with broader audience coverage.**

The problem is that most of these posts feature outrage, violence, and vitriol which became a propaganda operation's dream. It was exactly this tech feature that allowed malignment content to get repeated so so often to online audiences. The propogandists understood that digital marketing monetized legit content right alongside content designed to distort perceptions, deceive audiences, and destroy the civil bonds that heretofore created social order. This is exactly what they leveraged to full effect.

4. Verification is MIA. The digital adtech business model is antithetically opposed to any type of verification that may reduce advertising ad placements and thus revenue. **The lack of trust technologies was not an accident but baked right in from the beginning** to enable highly profitable scale media buys. From Facebook to digital data companies – impressions, clicks, viewability metrics, et al – defy virtually all attempts to verify what is real versus fake. Coincidence? Not a chance.

THE 'UNKNOWABLE DISTORTION FIELD' IS WHAT BROKE THE SOUL OF DEMOCRACY.

Taken together, it should be obvious at this point that there is a direct link between digital marketing technology's detachment from verifiable reality to the 'Unknowable Distortion Field,' a space where truth becomes impossible to verify and the resultant, catastrophic assault on democracy we all see before us.

The consequences are equally obvious. The flood of disinformation had the intended effect of sowing discord among different groups and trapping the public within the 'Unknowable Distortion Field' — a state of confusion that ultimately pushed democracy to the brink. Now, too many of our citizens live in the perpetually stressful world of the unknown - populated with boogey men and deep state actors ready to pop out at any time to turn their world upside down. This is especially tragic for younger minds, who become angry; angry enough to lash out.

The "scale' of the damage is that many citizens are trapped in a state of disempowerment and ultimately disenfranchisement that undermines the very foundations of democracy.

This is why it is 100% fair to place digital marketing tech at the center of the full-frontal attack on democracy. Digital marketing tech weaponized communication capabilities at scale – capabilities that simply did not exist 15 years ago.

THE TRUST WEB GETS US BACK TO REALITY.

The answer to dismantle the 'Unknowable Distortion Field' is simple if not easy. It lies in transforming today's digital marketing tech from a trust-starved web system into the Trust Web it was meant to be.

If we consider the Internet born in the 1990s to the Internet of today, we see a huge delta between the optimistic Internet in its early days and the trust challenged Internet we see today.

I am especially disheartened to see the ever-widening trust gap because I was literally in the room when the Internet happened, (https://trustwebtimes.com/in-the-room-where-it-happened/). I had an up-close view to the Internet's earliest days (circa 1994 – 2000) working at Lucent Technologies (hardware side) and Bell Labs (software side). My colleagues and I sensed that the Internet was possibly one of the most remarkable transformations in human history. It became a sacred mission, treated with great care as we were cognizant of the fact that the decisions, the technologies, and protocols we were developing would be far-reaching.

That's why when I juxtapose the Internet that should have been to what the Internet became, I can trace democracy's decline to a few destructive digital adtech monetization dynamics that drove the entire monetization machinery of the Internet.

The combination of misinformation/ shock content economy and the unverified web with its scale push engine inverted the Internet's earliest principled vision to democratize information distribution so that everyone had the potential to learn and tell their truths.

The tragic irony is that the same technology that democratized content distribution for everyone has become the primary driver of democracies' decline worldwide.

The key to restoring the Internet, therefore, is by embracing – not fighting – the content-serving DNA of the Internet through a verifiable model. Trust technologies and practices will eviscerate the 'Unknowable Distortion Field' because with trust-centered protocols, people have agency again. With clarity, doubt of everything unknown evaporates. People can decide what they think based on their perspective not because they are frozen in fear.

The emancipation of our democracy from digital adtech's grip is a multi-front battle to include advertisers (and their ad agencies), consumers, technologists, and – yes - politicians. Longer term, AI will play a positive role in all this – becoming the trust layer of the Internet where people can train their AI Agents to ferret out false information and provide verification of suspect content or profiles. An early example of how trust protocols can reinject trust into digital experiences is X's Grok feature which allows users to question claims made in posts.

This early example portends a future where new trust Agents help people decide how to contextualize what they think by being able to assess the trustworthiness of a source or content – for themselves.

The process to take power back from the digital marketing ecosystem requires everyone play their part; Advertisers, Ad Agencies, Technologists, Consumers, and Politicians.

ADVERTISERS:

- **Assume most of what is being bought in digital media is faked or fraud unless proven otherwise.** This is a dramatic stance but justified, nonetheless. Be relentless in making digital marketing tech providers come clean and accept the fact that verification firms have a financial incentive to keep the "unknowable scale" game going, (explained here – https://trustwebtimes.com/traffic-authentication-the-most-nettlesome-issue-in-ad-tech/). This is a painful step, but necessary if we want to weaken the potency of the 'Unknowable Distortion Field.'
- **Reject Typical Metrics to Evaluate Media Buy Success.** The standard metrics used in digital media buys regularly include metrics that are gameable and hard to verify. They also happen to be the business model columns holding up the digital media buying edifice:
    - CPM (the cost to buy a bundle of 1,000 impressions). CPM cost, especially low CPMs) matters too much in media decisions. Superficially, a media plan with a $10/ CPM sounds more efficient than a plan with $50/ CPM. Yet, obviously the lower CPM outlets could be a money loser compared to quality media where ads reach real audiences.

This is why advertisers should cease using CPMs as a metric determining media choices.

- CTR. In a perfect world, clicks do indicate interest but we do not live in a perfect world. Clicks in digital media ***can*** represent interest but the issue is that no one can know whether a click is from a real person or a bot or if the person is in the addressable universe.

  The lesson here is that CTR metrics give some information but it is of little real value because too much CTR data is too noisy data to be helpful.

CPM and CTR have become the metric proxy for media buying efficiency which is great for marketing tech firms (so little is verifiable) but not so great for advertisers. The take-away here is that advertisers should stop giving much weight to these metrics. Instead, the useful, key indicators should revolve around quality outlets that have value to real people and those outlets who can demonstrate delivering real outcomes.

- **Advertisers need to rethink which media outlets they support or don't support.** This is a moment to invest in media channels that cultivate trust such as local media and even radio.
- **Pay Agencies Commensurate to the Extra Labor for Direct Media Management:** In the process of recasting media buys, rethink how your ad agency is compensated for doing media buys that may require more labor.
- **Demand complete transparency** of where ads are running to ensure ad dollars are not supporting hate content.
- **Move to first-party data** versus third-party data as fast as your digital legs can run. Tracking people using third-party data not only violates users' privacy but creates the conditions for targeting abuse. Taken to an extreme, third-party data, as a category, ultimately, can be used to radicalize audiences.

AD AGENCIES:

- Push for full transparency with ad network partners so clients know what type of publishers their ads dollars are supporting. This is achingly difficult in programmatic channels, which may suggest agencies should refrain from or significantly reduce their investment in programmatic media – of all kinds.
- Execute more direct buys with quality publishers and reject scale media buys as the main media buying paradigm.
- Consider moving away from people targeting and pivot to topic-based targeted media buys. Allocate media dollars in a buy based on topics rather than profile by running in smaller publications or creating sponsored content media buys.
- A healthy digital ecosystem means ad agencies should think hard about their past or future investments in profile tracking capabilities, data, and practices. The black swan event in

data profile solutions is coming up fast because new AI Agents will be more proactive in protecting and managing users' online data and experiences.

Prepare now for this fast-approaching data horizon or else risk being weighed down with stranded data assets that are about as valuable as a buggy whip is today.

TECHNOLOGISTS:

The heavy lifting will, naturally, concentrate on tech trust tools and trust AI Agents. There is no need to dismantle the current version of digital marketing tech. Instead, in the decades ahead, the goal is to provide tools and technologies to introduce the trust layer into the Internet's infrastructure.

It makes sense that technologists must lead the migration to the Trust Web because digital technology is what dissolved our civic trust in the first place. Therefore, technology firms have a unique responsibility to pivot from extractive models where users are commodities to be monetized to a "Trust Tech" framework with a trust layer embedded in the user's digital experience.

The solutions outlined below focus on transparency, verifiable identity, user control, and the shift from tracking people to tracking intent.

The firms solving the problem of introducing trust into the opaque world of digital will come from three central players in the digital landscape: digital marketing, software tech providers, and browsers.

Each segment must introduce trust into the overall digital ecosystem at different junctures along the users' online journeys. Some approaches focus on digital marketing trust while other technologies are designed to provide users with tools to assess the credibility of content.

Taken together, these newer technologies will become pervasively embedded in everyday digital experiences. Most encouragingly, some of these solutions are already in progress.

1. Digital Marketing Tech Trust Building Tools:

A. AI-Driven "Topic Intelligence" Tracking – Not People

Rather than using AI to profile individual humans, firms can deploy deep learning models to analyze the "Topical Narrative" of audiences' content choices. This AI-driven approach identifies which topics have traction to convert audiences. By aligning brand messages with high-performing topics rather than following specific users around the web, brands can achieve ROI while respecting individual privacy.

An example of a technology platform that is a topic-centric targeting model is the Topic Intelligence platform. This data and analytics platform analyzes the prime topics a brand can activate to move people from content to conversion – all without tracking people. This provides high-level ROI that marketers need without ever compromising an individual's right to anonymity.

B. Navigating the "Topic Journey" for Users

The role of the new Trust Agent is that it allows users to participate in the digital economy on their own terms. Instead of being tracked by "creepy" behavioral markers, AI Agents share your intent but hides your identity. It could work like this. Imagine a user is looking for a new car. The Agent communicates your "Topic Interest" to a search engine and allows the ecosystem to show you relevant ads for cars. The moment you close that tab, the Agent "seals" that intent. It prevents brands from following you across the web. Intent driven by users drives the action – not a brand's trying to "target" you in every digital moment.

C. Blockchain-Verified Ad Supply Chains

I know, I know - about 10 years ago blockchain landed on the digital marketing landscape with a lot of hype and highfalutin promises but then quietly faded into oblivion a few years later. The problem was that the main application back then was around media buying/ selling, which blockchain was wholly unsuited to process.

Now, blockchain has a far more useful and nuanced application: to plug up one of the biggest leaks in the media buying "trust pipe" - ad fraud. While the nature of adtech fraud can take various forms such as fake profiles and clicks or "made-for-advertising" (MFA) sites, by using a decentralized ledger (blockchain), tech firms can tackle the fake profile problem. Since blockchain provides a transparent, immutable record of every ad impression, blockchain can be used to ensure brand budgets are actually going to legitimate publishers and "audiences" that are real humans, not bot farms. Combining blockchain with AI will be like aiming a double-barreled shotgun at adtech fraud. It is not, literally, a silver bullet but it is likely to put a huge hole in adtech fraud.

SUMMARY: Digital Marketing Tech Trust Building Tools.

The digital marketing ecosystem has much to atone for when it comes to a personal loss of control and agency. It is fitting, therefore, that to get to a Trust Web requires a rethink of how digital marketing firms make money. This is a tall ask but the prize is a healthier digital landscape where users are safe and democracy is safe too.

Comparison of Traditional vs. Trust-Based Ecosystems

Feature	Traditional Marketing Tech	Trust Technology Ecosystem
Data Focus	Tracking People (PII)	Tracking Topics & Intent
Privacy	Opt-out (Complex)	Privacy by Design (ZKP/DID)
AI Usage	Behavioral Manipulation	Predictive Performance / Sentiment
Accountability	Opaque "Black Box"	Verified Provenance & Ledgers
User Agency	Passive Data Source	Active Data Steward

2. Digital Experience Trust Building Tools (Software) for Everybody.

In a digital landscape often marred by misinformation and invasive tracking, a new generation of "Trust Tech" is emerging to restore the foundational security to the everyday user. These innovations; ranging from decentralized identity wallets to verified content provenance, are part of the trend to move the focus away from individual surveillance and toward verifiable transparency.

The focus in this section is outline how to tackle the deepening crisis of mass psyops campaigns through content distribution technologies. The approaches tackle different aspects of this problem but the goal is to help people combat all the digital content bullets assaulting them every day.

Ultimately, these technologies give users armaments needed to protect the shared democratic narrative from malignant actors and systemic manipulation.

A. Content Provenance and Digital Watermarking

To combat deepfakes and misinformation, tech firms are adopting the C2PA (Coalition for Content Provenance and Authenticity) standard. By embedding tamper-evident metadata or digital watermarks into assets, companies can provide a verifiable "origination story" for every piece of content. This allows users to take control with click to a "Verified" badge in their browser to see who created the media (for more on this, see content verification in the next Browser section).

The proactive power for users in this approach lies in the AI Trust Agent, which acts as a real-time fact-checker and provenance scanner. This Agent automatically inspects metadata across images, videos, and news articles, flagging content that lacks a verified history. In the future, these Agents could even provide a "Predictive Score" to help users distinguish authentic discourse from propaganda or destructive actors. Applying this scoring technology to images and videos will be incredibly important.

B. Personal AI Trust Agent (PAITA)

A personal AI Trust Agent acts as a sophisticated digital "buffer" between an individual and the often-predatory digital ecosystem. Instead of a person navigating the web with its invasive surveillance practices, the AI Agent serves as a locally hosted, private intelligence layer that evaluates every interaction, data request, and piece of content before it ever reaches your eyes or your device’s storage.

The Personal AI Trust Agent (PAITA) functions across the digital world using an Identity Gatekeeper, a.k.a. the "Zero-Knowledge" Bridge.

Instead of handing over your email, location, or age to every website you visit, the Trust Agent manages your Decentralized Identity (DID). Technically, when a site asks for your data, the Agent uses Zero-Knowledge Proofs to verify you meet the site's requirements (e.g., "Yes, this user is a resident of New York") without revealing who you actually are. It effectively ends the practice of creating "shadow profiles" by ensuring the data remains on your hardware, not the brand's server.

C. Autonomous Permission Management

Most of us agree to Terms of Service without reading them because, well, why bother. They seem to be deliberately long and obtuse and hard to understand. Sites know this and count on our inability to proactively make sense of it. This is exactly where AI can be hugely impactful. An AI Agent can scan these legal documents in milliseconds and summarizes the "trust cost" of using a service.

More than that, the AI Agent can provide a 'Trust Score' for apps and websites. If an app's 'BAU' (business as usual) involves selling your location data to third party firms, the Agent will automatically block those specific protocols or alert you that the 'trust protocols' of that service are compromised.

D. Localized Intelligence For Federated Learning

Today, all your searches, AI chats, and preferences are “logged” into the big brain of mega data companies. Imagine, instead, a way for an Agent to learn your specific preferences and values, but the data stays local. This is “Federated Learning” in action and it improves your experience without ever uploading your personal habits to a central cloud.

Your Agent learns that you prioritize medical privacy over shopping convenience. It then automatically hardens your browser settings when you visit health-related sites, ensuring that sensitive data is never leaked to data brokers. This allows AI models to "learn" from data directly on a user’s device (like a smartphone) and sends only the "lessons learned" back to the website the user is interacting with. The paradigm shift is that raw, personal data never leaves the user's possession while still allowing for "smart" optimization that people want without the centralized data risk.

E. Decentralized Identities

Related to the point above, the idea of digital wallets is readily understood by many people, however, the concept here moves digital wallets into new territory. Tech firms can move away from "Login with Google/Facebook" and toward Decentralized Identity that allows users to carry a digital "Identity Wallet" they own and control. When interacting with a brand, the user chooses exactly what data to "unlock" for that specific interaction. When the transaction is over, they "relock" their data, preventing the brand or third-party trackers from following them across the rest of the digital ecosystem.

SUMMARY: Digital Trust Building Tools for Everybody.

The digital marketing tech has taken away our fundamental right to online agency or the right to make independent, informed choices for ourselves.

Therefore, the future must lie with replacing digital experiences managed by whatever site a user finds themselves on to a model where the user is in control – at a deep and profound level. By recognizing agency as a fundamental digital right, we can rectify the systematic disenfranchisement of users by the for-profit digital tech sector.

In practice, this represents substantive shifts in the digital experience of users today versus user experiences in the future. The ultimate tech shift lies in who is controlling the user experience.

Today, external companies decide everything for audiences – what ads they see, what data is shared, what content is valued. Tomorrow, users themselves will be drivers of what happens to them online.

Comparison of User Control Models

Feature	Legacy Browser Model	User Activated Trust Model
A. Content Provenance	"See it and believe it"; vulnerable to deepfakes and misinformation.	Uses tamper-evident metadata and AI scanning to verify the "origination story" of media.
B. Identity & Privacy	Stored on platform servers; creates "shadow profiles" via data harvesting.	Keeps identity on local hardware, using Zero-Knowledge Proofs to verify traits without revealing personal ID.
C. Permissions	High-friction "Opt-out"; obtuse Terms of Service meant to be ignored.	Automatically summarizes the "trust cost" of legal docs and blocks invasive tracking protocols in real-time.
D. Intelligence	Centralized in the "Big Brain" of mega-data clouds; habits are logged and sold.	Utilizes Federated Learning so models learn from your habits locally without raw data ever leaving your device.
E. Data Sharing	Permanent access; "Login with Google/FB" allows persistent tracking across the web.	Employs an Identity Wallet to "unlock" data for specific transactions and "relock" it once the interaction is over.

3. Browser Activated Technologies.

Browsers serve as the "front door" to the Internet, making them the most powerful point of entry for restoring digital trust especially as the data landscape shifts from the "Wild West" of unregulated scraping toward a more accountable ecosystem.

The browser and the child industry of data providers must evolve from being data aggregators that put 'people' up for sale to being ethical stewards of user data.

Browsers and data providers are adopting specific frameworks that prioritize transparency and human agency. As noted above, this means moving away from controlling of user experiences toward making users in control of their own experiences.

A. On-Device Personal Data Vaults and Privacy Sandbox

> We saw above that, on the consumer side, what a personal AI Trust Agent would do. Browsers' role would be in coordination with PAITA. In practice, an AI-driven Personal Data Vaults combined with a Privacy Sandbox functions as a decentralized security architecture that shifts data ownership from corporate servers back to the individual.

In this ecosystem, the Personal Data Vault acts as a locked, encrypted repository stored on the user's own hardware or a private cloud, containing all sensitive information like browsing history, biometric data, and financial records.

The AI-driven Privacy Sandbox creates a "clean room" environment where data exchanges occur locally. This acts as a sophisticated intermediary, processing third-party requests and providing only the specific, anonymized answers required. Within this construct, when a website asks for "targeting" information, the browser provides a generic "interest token" (e.g., "User likes hiking") without ever revealing the user's identity or specific browsing history. This allows for relevant experiences without the underlying "creepy" surveillance. More important, the raw data never leaves the user's possession.

B. Granular Permission Dashboards (The "Trust Cockpit")

Currently, most browsers offer an "all or nothing" approach to privacy (like Incognito mode).

A trust-focused browser would provide a 'Trust Cockpit' — a centralized dashboard that shows exactly what every site is trying to do in real time.

The basic concept is that the browser would allow users to be different online profiles for each session. For example, when in business mode, the browser would suppress non business content. If one is browsing as a parent, the browser would present a bias toward family-oriented content and commerce.

Taken further, the browser would provide a Data Nutrition Label for every site and in every user persona. Users could use "kill switches" to instantly revoke a site's access to their microphone, location, or "topic history" with a single click, effectively acting as a personal firewall against bad actors.

C. Provable Content Provenance and Chain of Custody

The role of browsers in cleaning up the content mess lies in transparency regarding the content supply chain or provenance of content. These labels disclose exactly how content was created so there is a transparent audit trail that proves the content was published by legitimate sources rather than through overt actions of bad actors. It also would disclose which AI tools were used to edit it, and if it has been altered since publication.

There is an obvious challenge with this type of mechanism which lies in understanding the technology needed to label a source legitimate versus a bad actor without infringing on free speech rights. This is not a small issue, but longer term, a content Nutrition Label can serve as a red flag that the content was the product of unethical players. The key lies in giving users information that allow them to assess the veracity of content being presented.

D. Implementation of Privacy-Preserving Technologies

Data providers will need to move away from selling raw profile data and instead sell insights generated through privacy-preserving technologies. Methods like "Differential Privacy" or "Synthetic Data Generation" allow providers to share the statistical "truth" of a dataset without ever exposing the real-world identities of the people within it. This is not easy to achieve as we all learned with the Google's failed attempts to kill the cookie from 2020 to

2024. The game changer this time is AI's ability to give control back to users. That substantial change – changes everything.

SUMMARY: Browser Activated Technologies.

The shift in data ethics is a major transformation for how data is harvested, managed, and monetized. For the last 15 years, data was ruthlessly harvested often without users' permission. Going forward, the shift is toward overt user management of their digital profile data.

Comparison of User Control Models

Feature	Legacy Browser Model	Trust-Agent Browser Model
Identity	Stored on platform servers	Stored on user's local device
Tracking	Passive and invisible	Transparent and revokable
Media	"See it and believe it"	Verified via digital provenance
Data Sharing	High-friction "Opt-out"	Low-friction "Trust Cockpit"

CONSUMERS:

In the content tsunami, one thing is of paramount importance: people were all too willing to outsource their thinking. De-stabilizing the 'Unknowable Distortion Field' will happen one person at a time as they adopt new trust technologies in everyday life. Just as SSL (Secure Socket Layer) in the browser window trained people to look for the padlock to ensure digital transactions were encrypted, people should adopt trust protocols as fast as possible. Until tech catches up, here are some practices you can adopt right now:

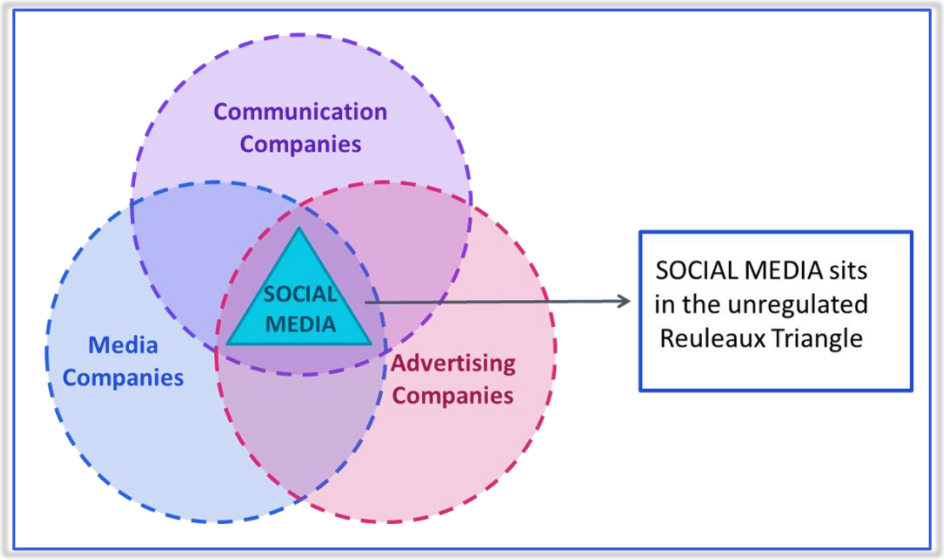
- Don't consume news via social media as that eliminates the context of the information.
- Do not expect "news" to be neutral – it is not. The goal is to get a variety of news inputs and compile a balanced view for yourself. Media can't provide this level of impartiality anymore.
- Use ad blocker browsers that don't track you like Brave, Mozilla Firefox or DuckDuckGo.
- Your phone is like the heart of your digital soul so care for its health as rigorously as your real heart. Avoid unhealthy apps and exercise your phone's settings to optimize privacy.
- Pay attention to the opt-in tracking choices on websites. They are often engineered to fool you into agreeing to be tracked when the reverse is true. Take the 30 seconds to read the options and choose with care.

- The paradigm of content is free on the Internet is exactly the root cause of the proliferation of dark content factories designed to deceive. Be willing to support quality content outlets with subscription fees. Yes – money. Free content is never really free – it is just hard to quantity the cost in free outlets. Pay for local news. Subscribe to Substack outlets you think are worthy of support. Whatever media outlets you choose to support – please, please do not trust "news" you get on social media. It is about as trustworthiness as a tabloid journalist who is only interested in getting paid to submit juicy, probably false, stories.

POLITICIANS.

There is an urgent role politicians must play here too. It seems politicians have a general attitude of surrender when it comes to digital marketing tech oversight, thinking they cannot be regulated. This is only partly true but with imagination, there are political mechanisms to bring digital marketing platforms to account. The place to start is with social media platforms.

Cleverly, social media's successful oversight avoidance strategy lies in the fact that they occupy the unmonitored Reuleaux Triangle; the intersection of communications, media, and advertising industries.



This regulation-free zone keeps social media beyond regulatory reach while simultaneously giving these firms benefits not available to any business segment anywhere:

- Social media is free to monetize the "network effect" of a communications company without paying any relevant taxes that communications firms must pay.
- Social media can monetize content like a media company through ads, yet they don't have any of the high human costs to create trusted content with verified facts.
- Social media has pulled off the greatest data heist of all time, unabashedly harvesting vast amounts of personal data to sell to the highest bidder without any concern for the data's use.

Social media platforms escape scrutiny and accountability hiding under the banner of “free speech.” This provides lots of cover for many irresponsible behaviors to flourish. We all understand social media has no intention of changing its business model, so, it would seem that no one or nothing can fix some of the worst abuses of social media. This, it turns out, is wrong. In fact, the “fix” may be easier to manage without complex oversight or sketchy regulations for social media platforms.

THE POLITICAL FIX THAT CAN WORK IS BY GETTING REAL.

Salvation can come from the very thing that politicians are good at – levying taxes. Fixing social media means forcing social media out of their safe, unmonitored Reuleaux Triangle and into the domain where taxes can be assessed for every verified user managed by digital marketing tech.

Specifically, the government can tax every live, active account with a tax similar to the Universal Service Tax that is levied on communications network companies for every live telecommunications account they service.

This approach will incentivize these networking platforms to delete fake accounts instead of monetizing as many accounts as possible. Better yet, this approach solves lots of problems at once:

- This approach doesn’t require social media to be trusted to adhere to “bespoke” regulations that would be hard to police anyway.
- It forces digital media to reckon with the real cost of fake/ troll accounts that pervade its platforms since each fake account will now cost them money.
- It deconstructs the scale monetization formula of social media who rely on large audiences of “accounts” with no responsibility for the damaging content that is continually spewed out by all these “accounts.”
- It can be done in a bi-partisan way quickly since assessing taxes is one thing politicians know how to do, and they don’t have to understand social media to do it.

By zooming in on social media, politicians can start to fix the abuses because social media is a super spreader of unverified information. Starting with social media means we are confronting the reality that social media, in particular, stole our ability to know who to trust or what to believe.

REAL WORLD CONSEQUENCES THE TRUST WEB REMEDIATES.

Conclusion:

Ultimately, restoring the "trust glue" in our digital world cannot be achieved through a single policy or a standalone piece of software; it requires a coordinated, multi-front offensive across the entire technological spectrum. From digital marketing shifting toward privacy-first topic tracking and content providers adopting ethical digital watermarking labels to browsers and personal AI Agents acting as vigilant gatekeepers for the individual, every layer of the ecosystem must evolve.

Different tech companies are tackling the problems from different angles but one thing remains clear. By equipping users with the tools to verify the "origination story" of profiles they encounter

online, content they see and data they share, we move away from a system defined by "unknowable" villains and toward a transparent architecture of accountability. Only through this collective realignment can we safeguard our shared narrative and ensure that the future of the web is built on a foundation of verifiable truth rather than systemic manipulation.

Unless we pursue this path, we will continue to be let down by the key stakeholders in the digital tech ecosystem. These companies should have been the guardians of our digital souls, protecting advertisers and audiences alike but instead, they chose profit over trust and revenue over responsibility. This failure was directly responsible for a digital marketing business model which proved easy to exploit by malicious groups capable of rapid, large-scale disruption.

This is a classic case of a free, capitalistic market that threw all guardrails of trust verification protocols out the window in the name of profits. As a result, culture wars meshed with identity politics into a combustible, destructive concoction that is easy to ignite but hard to quell.

The Internet is overflowing with too many bots and trolls and content all designed to push untrusted agendas. The indisputable and destructive role of digital marketing tech in this toxic brew is that it made it so easy for anyone with hands on keys to reach many people, utterly undermining our ability to trust anything. All political debates have been reduced to a winner takes all zero-sum game pitting neighbor against neighbor and brother against brother, sapping our energy, leaving us all deeply pessimistic about our future – in the real world.

The 'Unknowable Distortion Field' is the manifestation of a tech ecosystem gone rogue, wreaking havoc on a global scale. Salvation comes with nextgen digital marketing tech firms powered by AI because AI can be molded into a "trust force" capable of dismantling the 'Unknowable Distortion Field.'

Once trust tech dominates the Web again, we can construct The Trust Web as it was meant to be, ushering in a digital renaissance age that awaits us all.

Trust in that.

About the Author: Judy Shapiro is a marketing veteran who has developed new technology and practices for performance marketers. She is CEO and co-founder of Topic Intelligence, a data company for acquisition marketing and engageSimply, a service company to plan and deploy acquisition marketing.

She also founded The Trust Web for new business model in adtech that serves consumers, advertisers and publishers.

Judy's experience includes large ad agency (NWAyer), large companies (AT&T, Bell Labs, Lucent Technologies) and technology security companies (CA, Comodo) which has given her a deep and broad perspective which she shared in outlets like Ad Age, HuffPo, Digiday, Crain's, and Business Insider. (Muckrack Profile: https://muckrack.com/profile/portfolio)

General, Media and Press Inquiries: Judy Shapiro | judyshapiro@engageSimply.com