# Tech Industry and the Avoidance of "Techlash"

*A Sensible Approach to Regaining Trust on the Internet*

March 2020

# Synopsis

In 2018, WITSA published a policy statement[1] seeking to address some of the most worrisome misconceptions and threats to the multilateral trading system that has served the ICT industry as well as all other industries, citizens and consumers so well in modern times. Growing animus toward "Big Tech" companies and generalized opposition to technological innovation is threatening industry development and economic growth by engendering support for policies that are expressly designed to inhibit it. That is deeply problematic for future progress, prosperity, and competitiveness.

The concerns being raised about the technology industry, in particular large tech companies are not all frivolous or without merit. This paper's intention is to debunk the main misconceptions that are associated with this "techlash" and identifies several recommended actions and policy principles which WITSA believes can rekindle faith and trust in the technology industry for the betterment and delivery of the promise of the digital Age where everyone on earth benefits from the use of ICT.

As with other technologies of the past, as digital technologies have matured and new innovations continue to emerge, we are continuously confronted with new challenges to maximize the benefits and minimize the harm inflicted by them. As in previous era, appropriate policy responses in time will be developed to foster industry innovation, competitiveness and consumer welfare for the betterment of society and for our future prosperity.

[1] Globalization: Perception vs. Reality: Why Opposition to International Trade and Open Borders is Misplaced, Counter-Productive and Harmful to Our Future Security and Prosperity : https://witsa.org/wp-content/uploads/2018/12/Globalization-Perception-vs-Reality_final.pdf

# Context

***Over the past few decades, innovation in Information and Communications Technology (ICT) has brought about untold benefits and transformed millions of lives in amazing ways***. ICT has helped create new job opportunities by making labor markets more innovative, inclusive, and global. Rapid advances in digital technology are redefining our world. The plummeting cost of advanced technologies is revolutionizing businesses, industries, governments and society. And the 'combinatorial' effects of these technologies – mobile, cloud, artificial intelligence, sensors and analytics among others – is accelerating progress exponentially. ICT provides users with unparalleled opportunities for value creation and digital technologies are creating new profit pools by transforming customer expectations and how companies can address them.

***However, in recent years, a backlash we will call "techlash" has emerged; marked by an increasing enmity towards large Silicon Valley platform technology companies.*** For many years, Silicon Valley was characterized by techno-optimism, a belief that technology can continually be improved and can improve the lives of people, making the world a better place. A dramatic turnaround has taken place with the revelation of election manipulation, personal data collection abuse, misleading and false information, hoaxes and "fake news" – with all becoming too commonplace in social media.

***In March 2019, Facebook CEO Mark Zuckerberg went as far as to call on regulators to play a "more active role" in establishing rules of the Internet, and in particular "stricter regulation of harmful content, election integrity, privacy and data portability"[2].***

Large Tech companies are also facing scrutiny from an anti-trust and competition angle. The US as well as other national regulators are questioning whether companies like Amazon, Apple, Google, and Facebook have too much power. Led by prominent political figures, including candidates for the U.S. Presidency, this new push to curb the power of Big Tech has a catchy solution: break up the companies. But a breakup will be hard to force, and the history of trustbusting suggests that many other solutions are possible.

## Is the Techlash Over-Hyped?

The answer is yes and no. The scale and loudness of the current techlash means it must be taken seriously and addressed with measured, thoughtful and considerate responses. Opposition to new technologies and the industries that are formed around them is nothing new. At various times throughout history, technology pessimists have opposed innovations as harmful, including electricity, machines, automobiles, elevators, recorded music and the telegraph, among countless other technologies we now take for granted.

***The first step for tech industry is to acknowledge that today's backlash originated at least partially from real events and represent real systemic challenges that society as a whole must address, including privacy and cybersecurity among other concerns.*** A major impetus for today's techlash was the disclosure that Russia utilized social media platforms to interfere in the 2016 U.S. Presidential

[2] Washington Post Op-ed March 30, 2019: https://www.washingtonpost.com/opinions/mark-zuckerberg-the-internet-needs-new-rules-lets-start-in-these-four-areas/2019/03/29/9e6f0504-521a-11e9-a3f7-78b7525a8d5f_story.html

elections and that Cambridge Analytica obtained and illegally used personal data from over 87 million Facebook users for political influencing. Another matter is the ongoing antitrust investigations regarding Google, focused on the tech giant's online advertising and search traffic.

Nevertheless, consumers around the world continue to take advantage of emerging technologies and social media usage is increasing, not decreasing[3]. Public opinion is still largely favorable towards information technology and communications companies***. According to Edelman's 2019 Trust Barometer, a significant majority of people around the world (78 percent) remain trusting of ICT companies and that the technology sector is the most trusted of all industry sectors globally[4].***

***However, trust in social media platforms and in search engine companies, in specific, are in decline: According to the 2019 Trust Barometer, trust in social media and Internet search companies has diminished significantly over the past year. As our understanding of the nature of these problems grows, so too does demand for a coordinated and comprehensive response from governments, civil society and the private sector.*** But while there is growing recognition of the problem, there remains significant ambiguity and uncertainty about the nature and scale of the appropriate response. Democratic governments around the world have, therefore, begun to search for strategies to govern the digital public sphere. Many are converging on what might be called a platform governance agenda.

# Issues & Principles

## Anti-Trust and Competition Concerns

Companies such as Amazon, Google, Twitter and Facebook now span the globe by serving billions of users. By one measure, 70 percent of all Internet traffic world-wide flows though Facebook or Google servers[5]. Amazon is the world's largest ecommerce retailer, projected to encompass 47 Percent of online sales in the U.S. in 2019 and a growth rate of over 20 percent. Apple in August 2018 became the first public company to be valued at $1 trillion, followed closely by Amazon at over $900 billion and Google and Microsoft each valued at over $800 billion.

According to critics, all this leads to massive conflicts of interests, enabling Google to promote its own products in search results, and Amazon to give its own products preferential treatment on its ecommerce platform. Critics also accuse Facebook of stifling competition and hindering upstarts and innovation by locking in its 2.4 billion users, and criticize Apple of taking a commission from app developers and restricting them from selling elsewhere.

---

[3] "Social Media Fact Sheet," Pew Research Center, June 12, 2019, https://www.pewinternet.org/factsheet/social-media/

[4] "2019 Edelman Trust Barometer," https://www.edelman.com/sites/g/files/aatuss191/files/2019-04/2019_Edelman_Trust_Barometer_Technology_Report.pdf.

[5] Cuthbertson, Anthony. 2017. "Who Controls the Internet? Facebook and Google Dominance Could Cause the 'Death of the Web.'" Newsweek, November 11. www.newsweek.com/facebook-google-internettraffic-net-neutrality-monopoly-699286.

Underpinning the growth of BigTech is a massive collection of user data across services, which enables the social media platforms to improve tools and increase value through network effects, the principle that the more members or users a social network has, the more attractive it becomes for other people to join as well, because the usefulness of the network goes up with the number of users (commonly known as "the network effect"). Would-be competitors are at disadvantage because of the winner-takes-all dynamics and competition based on ecosystems leading to concentration of markets and competition concerns.

In the U.S., in 2019, the U.S. Justice Department and the Federal Trade Commission (FTC) launched investigations against Facebook, Google and Amazon for possible breaches of anti-trust law. Separate antitrust probes by 48 U.S. States, the District of Columbia and Puerto Rico were launched in September 2019 against Google and Facebook to determine whether their actions mishandled consumer data, reduced the quality of consumers' choices or increased the price of advertising. Senator Elizabeth Warren, a former 2020 U.S. Presidential candidate pledged to spin off Instagram and WhatsApp from Facebook and prohibit platforms like Amazon from both offering a marketplace for commerce and participating in that marketplace. Amazon would be required to divest itself from Whole Foods, and Google from Waze.

In the EU, three cases have been brought against Google related to its ads network, shopping search results and bundling of its apps on Android phones. The German competition authority in February 2019 ruled that Facebook can't automatically track its users on other websites or merge users' WhatsApp and Instagram data with their Facebook data, but must give them a choice instead. Over the past three years, Google has been fined $9 billion by European regulators (these fines are currently under appeal). This was followed in December 2019 by the U.K. Competition and Markets Authority (CMA) interim report on digital advertising markets, making a case for how to regulate Google and Facebook[6].

"Big tech companies provide benefits that are often overlooked, such as higher wage jobs and benefits than smaller companies can usually offer, more exports and more innovation."

***WITSA is of the opinion that the bigness of tech firms in of itself is not a problem.*** Many tech firms are large and have earned significant market shares. However, big tech companies also provide benefits that are often overlooked, such as higher wage jobs and benefits than smaller companies can usually offer, more exports and more innovation. Not to be overlooked is the fact that network effects and scale is a key component to maximizing the value that consumers need and demand. These companies are also platforms which have enabled new businesses and thereby created new jobs. Additionally, tech companies are major contributors to research and innovation, that drive market innovation, competition and development. In 2017, the top 5 spenders on research and development were all technology companies, with Amazon alone spending more than $22 billion[7].

Over time, open, competitive markets have proven best at delivering innovation, productivity and opportunities. Such markets have allowed these multisided, digital platforms to become key players in the digital economy, generating numerous user benefits by lowering transaction costs, introducing new

[6] https://www.publicknowledge.org/blog/shot-across-the-pond-uk-competition-authority-makes-the-case-for-how-to-regulate-google-and-facebook/
[7] https://www.politico.com/magazine/story/2019/03/13/dont-break-up-big-tech-225808

products, enabling new types of transactions and improving the "match" between parties to an exchange. Platforms facilitate value generation from previously under-utilized resources, thereby expanding the economy. The substantial economic value to users of "free" platform services is difficult to quantify and is disregarded in traditional measures of economic activity, such as gross domestic product (GDP) – though one can capture licensing revenues and devices sales.

The well-established consumer welfare standard in U.S. antitrust regulation requires the government to demonstrate that a merger or other action is likely to raise prices or reduce innovation before blocking it[8]. Although this policy protects both consumers and workers, it does not protect competing companies unless the activity is clearly anti-competitive. Nor does it attack size per se, recognizing that in many cases, larger firms are more efficient, leading to lower prices or more innovation.

While politicians around the world are increasingly calling on regulators to break up the largest Internet companies, break-up cases are by far the most difficult type of antitrust action and should be avoided whenever possible. There have been relatively few attempts, and none has produced ideal results. Separating various activities, skills and personnel into two or more viable companies is much harder than it sounds. Furthermore, regulators must remain engaged in how the various entities deal with each other and prevent one or more from capturing too much of a new market (It should be noted that regulators often have different definitions of markets leading to very different analyses of market power. In some cases, competitive players are ignored as not being in the same market by some definition).

***The classic danger from a monopoly is the tendency to lower supply, reduce innovation, and raise prices. Yet internet companies offer many of their most valuable services without a fee. Rather than cut supply, they continually seek to attract users with new services and products. The free use of these services has delivered tremendous consumer benefits.*** Perhaps most importantly, these companies have become major sources of innovation. For example, Amazon and Google spend more on research than any other company in the world; Microsoft and Apple are sixth and seventh respectively; and Facebook is 14th. When competition is based on innovation, not prices, it is a major driver of technological progress.

Moreover, despite their large size, large technology companies are more vulnerable to competition than is sometimes apparent, whether from similar markets, new entrants or foreign competition. Some are also denied access to markets, such as China. As antitrust experts Carl Shapiro and Hal Varian put it, "the information economy is populated by temporary, or fragile, monopolies. Hardware and software firms vie for dominance, knowing that today's leading technology or architecture will, more likely than not, be toppled in short order by an upstart with superior technology[9]." Because their business models are centered around data, the threshold for customers switching from one platform to another is substantially less than in the previous era that was dominated by tech giants such as IBM, Dell and Microsoft.

When all you have is a hammer, everything looks like a nail. The internet giants raise a number of important public policy questions besides antitrust. These include data privacy, censorship, and political influence. All of these issues require careful balancing of costs and benefits. Antitrust policy is simply not

[8] https://cei.org/blog/antitrust-basics-rule-reason-standard-vs-consumer-welfare-standard

[9] Carl Shapiro, Information Rules: A Strategic Guide to the Network Economy Harvard Business Review, 1998.

equipped to deal with such diverse issues. Properly understood, it does one thing: curbs threats to markets. Other issues demand their own policies, which should operate separate from antitrust (see sections below).

As has been found in extensive research by organizations such as the Organization for Economic Cooperation and Development (OECD), and the World Economic Forum (WEF), competition law in most of the world's leading markets include broad, open-ended rules that can be applied to a wide range of market practices, including those of large technology companies. Upending these established competition law frameworks therefore are unwarranted as they are mostly adequate. Instead, competition authorities should look at their existing enforcement mechanisms and avoid creating new rules for the digital sector which are either unclear or relies on ambiguous or underdeveloped concepts.

Before governments initiate a time-consuming and costly trust-busting crusade, they should begin with a competition policy agenda that delivers immediate, tangible results. Broader antitrust questions, if they are to be addressed, most likely require a collaborative international effort. ***New forms of antitrust oversight are needed for the digital economy that look not just at price increases to judge market power but also at control over data, constraints on innovation and reduction in consumer welfare[10].***

International cooperation and consensus-building efforts which are currently being undertaken by multilateral organizations such as the OECD, the United Nations Conference on Trade and Development (UNCTAD)and the International Competition Network (ICN) should be supported by all stakeholders. Since issues regarding big tech are often cross sectoral, ranging from competition concerns to privacy rights and data security, any new frameworks under consideration should also be based on cross-institutional cooperation whenever possible.

A greater harmonization of principles and rules of competition law would offer better predictability and lower the thresholds for market access for tech businesses who currently have to comply with over 130 different national competition regimes.

WITSA believes the following policy principles can best address many of the current antitrust and competition concerns regarding large technology companies:

## POLICY PRINCIPLES

**Current Antitrust Standards Work.**
Consumer welfare standard requires the government to demonstrate that a merger or other action is likely to raise prices or reduce innovation before blocking it. Although this policy protects both consumers and workers, it does not protect competing companies unless the activity is clearly anti-competitive. Nor does it attack bigness per se, recognizing that in many cases, larger firms are more efficient, leading to lower prices or more innovation.

**Breaking up is hard to do.**
Politicians around the world are increasingly calling on regulators to break up the largest Internet companies. Break-up cases are by far the most difficult type of antitrust action and should be avoided whenever possible. There have been relatively few attempts, and none has produced ideal results.

[10] OECD. 2018. Rethinking Antitrust Tools for Multi-Sided Platforms. Paris, France: OECD. https://www.oecd.org/daf/competition/Rethinking-antitrust-tools-for-multi-sided-platforms-2018.pdf

Separating various activities, skills and personnel into two or more viable companies is much harder than it sounds. Furthermore, regulators must remain engaged in how the various entities deal with each other and prevent one or more from capturing too much of the new market.

**Don't break what isn't broken.**
The classic danger from a monopoly is the tendency to lower supply, reduce innovation, and raise prices. Yet Internet companies offer many of their most valuable services for free. Rather than cut supply, they continually seek to attract users with more services. The free use of these services has delivered tremendous consumer benefits. Perhaps most importantly, these companies have become major sources of innovation. For example, Amazon and Google spend more on research than any other company in the world; Microsoft and Apple are sixth and seventh respectively; and Facebook is 14th. When competition is based on innovation, not prices, it is a major driver of technological progress.

**Not everything is a nail.**
The internet giants raise a number of important public policy questions besides antitrust. These include data privacy, censorship, and political influence. All of these issues involve trade-offs, requiring a careful balancing of costs and benefits. Antitrust policy is simply not equipped to deal with such diverse issues. Properly understood, it does one thing: curbs threats to competitive markets. Other issues demand their own policies, which should operate separate from antitrust.

**Data Portability***:* Social media platforms should strive to make Internet users' data portable, whereby customers of one digital platform are enabled to "port" their data to a rival digital platform. As with telephone number portability in the United States and other countries, or the concept of "open banking" in the UK, data portability gives customers a greater ability to "vote with their feet" and leave one company for a lower priced or higher quality rival. Industry should seek common standards, including a standard data transfer format such as being developed by the open source Data Transfer Project[11]. The Data Transfer Project is already supported by many of the key industry players, including Facebook, Twitter, Apple, Google and Microsoft.

**Data Interoperability**: Industry should seek "data interoperability," enabling different social media services to work together—for example by allowing users of one social media platform to post to another and vice versa (e.g. Instagram and Snapchat). This should be done via open standards, such as the W3C's social web protocols where appropriate, and allow open, federated services like Mastodon to work with social media platforms.

**Market investigations and industry collaboration must be improved**
Competition authorities are urged to work closely with industry and other stakeholders in order to compensate for their vast informational disadvantage, ensuring "participative trust" as well as long-term effective solutions. A more frequent use of market investigations would also make authorities more effective in addressing the dynamic and complex markets to restore competition.

**Broader antitrust questions require a collaborative international effort**
International cooperation and consensus-building efforts which are currently being undertaken by multilateral organizations such as the OECD, the United Nations Conference on Trade and Development (UNCTAD)and the International Competition Network (ICN) should be supported by all stakeholders. Since issues regarding big tech are often cross sectoral, ranging from competition concerns to privacy

[11] https://datatransferproject.dev/

rights and data security, any new frameworks under consideration should also be based on cross-institutional cooperation whenever possible. A greater harmonization of principles and rules of competition law would offer better predictability and lower the thresholds for market access for tech businesses who currently have to comply with over 130 different national competition regimes.

## Privacy Concerns

Some people equate big tech with "surveillance capitalism", the idea that pervasive data collection, including, but not limited to, tracking on websites, is eroding all privacy online[12] and, in some cases, offline. Following this viewpoint, Internet users, by subscribing to "free" services in exchange for access to their personal data, are little more than raw material fed into "machine intelligence" resulting in prediction analysis that use Internet consumers past and present behavior to anticipate future conduct.

Perhaps the most well now and troublesome privacy scandal in the Internet era was the revelation in 2018 that Cambridge Analytica – a relatively obscure U.K. political consulting firm – had harvested the personal information from over 87 million Facebook users without their consent and used it for political advertising purposes in the lead-up to the 2016 U.S. Presidential election. For this infraction, Facebook was fined $5 billion in 2019 and was ordered to create new layers of oversight for its collection and handling of users' data by the U.S. Federal Trade Commission (FTC).

"Much of the criticism directed at Big Tech is based on misunderstanding and exaggerations regarding how data collection is handled, and personal information is used."

Nevertheless, much of the criticism directed at Big Tech is based on misunderstanding and exaggerations regarding how data collection is handled, and personal information is normally used. Rather than "spying" on their customers, most companies are upfront about their use and dependency of customer data and customers mostly accept such free services fully aware that they are sharing personal data. For Internet users that do not wish to have their data collected, alternative services and technologies that do not collect personal data are available; e.g. the search engine DuckDuckGo is a viable alternative to Google or Bing. Google users can also take advantage of an anonymous ("incognito") mode for Google that results in no information being collected[13]. Additionally, some services can be provided for a subscription fee that is free of advertising.

It should also be noted that data collection is often a necessity for companies to improve their decision-making, productivity and product offering, such as customized services. As a result, participants are benefiting from cheap and low-cost services and are empowered by the services' data through device feedback loops – such as data from personal fitness, health and data tracking wearables to improve health.

[12] Shoshana Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power (Profile Books: London, 2018).

[13] https://support.google.com/chrome/answer/95464?co=GENIE.Platform%3DAndroid&hl=en

There are also widespread misconceptions regarding how customer data is commonly used by Internet companies. Rather than sell personal data to advertisers, Internet companies typically protects and retains this information while only selling or making available access to anonymized user information such as geographic location, interests, characteristics and behaviors. This is necessary to enable adequate targeting and advertisers can only access aggregate data and not personally identifiable data.

However, building and maintaining trust and confidence between all users of the Internet is one of the fundamental building blocks of the *Digital Age*. Trust and confidence are fragile concepts, often slowly formed, but rapidly destroyed when shown to be vulnerable, directly attacked or as an unintended consequence of other actions. All stakeholders have a role to play in building this trust ecosystem.

There is global concern about the adverse effect on trust and confidence arising from widespread commercial use of personal data, revelations of extensive electronic surveillance programs and efforts to undermine trust in ICT supply chain by governments, affecting both foreign and domestic citizens, corporations and individuals. This is additional to other recognized threats to the confidentiality, integrity and availability of information arising from hacking, fraudulent activities, viruses and other threats. Suggested responses by some governments, including proposals to localize ICT assets and server processing citizens' data within their jurisdictions, while superficially appealing, are nothing less than economic protectionism that threatens global growth. This localization also seriously diminishes the resilience of otherwise globally distributed systems.

WITSA advocates a principled approach, which recognizes information privacy as a fundamental human right, and seeks to balance this in context with equally important policy objectives of national security and data protection while maintaining the economic and social capability of digital information. This approach highlights the importance of transparency and accountability within appropriate legal frameworks, information sharing of risks and vulnerabilities, and collaboration across jurisdictions.

WITSA advocates the following policy principles:

## POLICY PRINCIPLES

**Privacy is a fundamental human value**
Every person on Earth should have a right to privacy and the ability to communicate anonymously, which means to control access to themselves and information about themselves that maintains their dignity, self-determination (the ability to know if and when the decisions one makes are being constrained or directed by external agencies), security, property and privacy, unless law requires otherwise.

**All countries should pass national privacy legislation**
All countries should pass national privacy legislation that is focused and includes provisions to ensure adequate enforcement against companies that violate privacy law.

**Targeted, substantial harms-based regulations and enforcement is preferable**
Furthermore, targeted, substantial harms-based regulations and enforcement can help policymakers pinpoint data misuse and make the aggrieved whole.

**Governments must openly acknowledge and codify the privacy rights of their citizens and residents**

Governments must openly acknowledge and codify the privacy rights of their citizens and residents, the importance of maintaining trust and confidence in the free flow of information Page 6 of 8 both within and across national borders, and avoid taking any actions that, without reasonable and specified cause, may undermine the confidentiality, integrity and availability of such information.

**Industry must promote transparency**
Industry must promote transparency about what data is collected and how it will be processed and handled, as well as promoting compliance with data protection, security and privacy laws, establish good industry practices, promote privacy by design in all products and services, and educate consumers about the purpose and benefits of data sharing.

**Effective privacy and data protection need a globally harmonized framework**
New privacy regulations around the world should build on the protections such as those provided in the European Union's General Data Protection Regulation (GDPR)[14]. It should protect your right to choose how your information is used — while enabling companies to use information for safety purposes and to provide services.

**No Forced Localization Measures Principle**
Government mandated Data localization requirements in the name of privacy create barriers to market access and must be minimized in order to promote inclusive growth regionally and globally. Data localization requirements are often the result of misguided attempts to protect local economies or for security or privacy reasons. Forced localization does not effectively strengthen privacy or security and are more often than not about data protectionism rather than data protection. Attempts to mandate localization of data can further escalate to internet balkanization.

## Disinformation and Election Integrity

Disinformation, AKA "fake news" is not new, and have tainted public discourse for hundreds of years, or even longer. However, in the digital era, false content has been amplified through social media platforms such as Facebook, Twitter, Instagram, WhatsApp, TikTok and YouTube by fearmongers, Internet trolls and election-meddlers to widen social fissures, undermine democracy and strengthen authoritarian regimes by spreading content that intends to deceive, mislead or manipulate.

In an attempt to tackle these challenges, in the first quarter of 2019 alone, Facebook disabled 2.19 billion fake accounts and took down 4 million hate speech posts and flagged 21 million cases of child nudity and sexual exploitation to authorities[15]. YouTube removed 2.8 million channels, over 8 million videos and 228 million comments from January to March 2019. Other platforms are working overtime to address similar problems with hateful and toxic content. Independent non-profit organizations, such as the EU DisinfoLab, are also focused on tackling sophisticated disinformation campaigns targeting governments, institutions, and core values by continuously monitoring disinformation activities the major digital platforms[16].

Disinformation and propaganda on social media platforms are an adaptation to the digital era of time-tested counterintelligence programs and strategies intended to sow discord and influencing elections.

[14] https://gdpr.eu/
[15] https://www.engadget.com/2019/05/23/facebook-2-billion-fake-accounts-disabled/
[16] https://www.disinfo.eu/publications

Such campaigns have already been waged in around 100 countries[17], seeking to influence elections in the Philippines (Rodrigo Duterte), India (Narendra Modi), Brazil (Jair Bolsonaro), the United States (Donald Trump), the 2016 Brexit referendum, and elsewhere. Other campaigns have contributed to calls for sectarian violence in India and Sri Lanka as well as genocide in Myanmar.

Tech companies are increasingly vigilant in fighting hate speech, fake news and election meddling on their social media platforms. Both Facebook and Google are now requiring political ads in the U.S. and in Europe to disclose who are behind them. Twitter and TikTok have banned political ads altogether and Google no longer allow political advertisers to target voters based on their political affiliation. Google's YouTube division, Facebook and others have also largely banned doctored videos and images known as "deep fakes". WhatsApp has implemented limits on the number of people or groups messages can be forwarded to. Moreover, companies like Facebook have developed artificial intelligence tools to combat non-permissible content. Most of Facebook's moderation is now done automatically. As much as 98 percent of terrorist content is now removed before anyone has the chance to see it, let alone report it[18]. Both Facebook, Twitter and Google have signed a voluntary agreement with world leaders, committing themselves to remove hate speech from their respective platforms.

It should be noted that technologies are not distinct from the people who use them but are extensions of ourselves. They will embody the biases that we apply through their design and usage. As fears about privacy encroachments and electoral interference increases, tech companies are tempting scapegoats.

"Rather than rushing to create a new framework for regulating speech online, and risk inadvertently harming legitimate speech or reducing the effectiveness of automated takedown mechanisms, policymakers should work with the private sector"

However, social media platforms such as Twitter, YouTube and Facebook were not invented to undermine trust in science or indoctrinate racists and extremists. Rather than rushing to create a new framework for regulating speech online, and risk inadvertently harming legitimate speech or reducing the effectiveness of industry's takedown mechanisms, policymakers should work with the private sector to improve such mechanisms, while ensuring platforms have moderation policies that protect free speech.

WITSA believes the following policy principles provide the best possible guidance with regard to addressing disinformation and election integrity on social media platforms:

**POLICY PRINCIPLES**

**Resist Regulations and Censorship:** With the exception of speech advocating violence or harm to other people, Governments should resist temptations to deal with offensive content and false news by forbidding or regulating it. Overly restrictive regulation of internet platforms in open societies sets a

[17] https://www.wired.com/story/the-two-myths-of-the-internet/
[18] https://www.technologyreview.com/f/614774/this-is-how-facebooks-ai-looks-for-bad-stuff/?utm_source=newsletters&utm_medium=email&utm_campaign=the_download.unpaid.engagement

dangerous precedent and can encourage authoritarian regimes to continue and/or expand censorship. This will restrict global freedom of expression and generate hostility to democratic governance.

**Human Intelligence Required:** The terminology and focus of the hate speech changes over time, and most fake news articles contain some level of truthfulness in them. Therefore, social media companies cannot solely rely on artificial intelligence or humans to monitor and edit their content. They should rather develop approaches that utilize artificial and human intelligence together.

**Prioritize takedown of harmful content:** To overcome the editorial challenges of so much content, companies should focus on a limited number of topics which are deemed important with significant consequences (e.g. the anti-vaccine movement causes more harm than the flat earth theory). Social media companies should convene groups of experts in various domains to constantly monitor the major topics in which fake news or hate speech may cause serious harm.

**Harmful content accountability and transparency:** Governments may hold Internet companies accountable for having systems and procedures in place to limit harmful speech, however, but should avoid setting specific performance targets or restrict specific forms of non-illegal speech. Measures to be followed may include channels for reporting content, external oversight of Internet companies' policies and enforcement decisions, as well as periodic public reporting of enforcement data in order to enable citizens and governments to assess progress in limiting harmful content on social media platforms.

**Modify & Review Recommendation Algorithms:** Social media platforms should consider if recommendation algorithms may inadvertently promote fake and hateful speech. Also, algorithms typically group users based on their shared interests and then promote the same type of content to all users within each group. Internet companies are encouraged to build transparency and user control on their platforms so that users can take control of what content are shown to them.

**Ban Violent & Criminal Content:** In rare instances of posts that incite violence or invite others to commit crimes, social media platforms should censor and ban the content with no hesitation.

**Educate, don't block**: While social media platforms should not be forced to block misinformation outright, they have a responsibility to call out fake news and disinformation without legitimizing them. They can do this by relying upon their in-house professionals and well-respected fact-checkers and by providing alternative information alongside the content with fake information so that the users are exposed to the truth and correct information. This approach has already been adopted by some platforms, including YouTube and Facebook. Social media companies cannot control how ideas spread offline. Unless individuals are presented with counter arguments, falsehoods and hateful ideas will spread easily, as they have in the past before social media.

**Governments should encourage independent, professional journalism**. The general public needs reporters who help them make sense of complicated developments and deal with the ever-changing nature of social, economic, and political events.

**Governments should avoid crackdowns on the news media's ability to cover the news**. Those activities limit freedom of expression and hamper the ability of journalists to cover political developments.

**Technology firms should invest in technology** to find fake news and identify it for users through algorithms and crowdsourcing. There are innovations in fake news and hoax detection that are useful to media platforms. For example, fake news detection can be automated, and social media companies should invest in their ability to do so.

**Funding efforts to enhance news literacy** should be a high priority for governments. This is especially the case with people who are going online for the first time. For those individuals, it is hard to distinguish false from real news, and they need to learn how to evaluate news sources, not accept at face value everything they see on social media or digital news sites. Helping people become better consumers of online information is crucial as the world moves towards digital immersion. There should be money to support partnerships between journalists, businesses, educational institutions, and nonprofit organizations to encourage news literacy.

# Conclusion

Throughout history, overly optimistic expectations and exuberance over the promises of new technology inventions, ranging from the Industrial Revolution -with its introduction to new, vastly more efficient manufacturing processes-, to the combustion engine and automobiles, inevitably gave way to disappointments and anxieties. Transformational technologies by definition are disruptive and carry with them unintended drawbacks as well as benefits. For example, the industrialization of the 19th Century was condemned by luddites and their "smash the machine" riots, by socialists and others. In the 1920s, a techlash against the automobile took issues with road safety, congestion and noise.

Techlashes of the past put the spotlight on the unintended consequences and harms that these innovations brought with them, leading to important new safeguards and remedies. For example, automobile safety enhancements, such as seatbelts, traffic regulations and airbags have dramatically reduced car accidents and fatalities. In a sense, a techlash can facilitate important discussions on how to best manage innovations and identify legal frameworks that limit their destructive potential while maximizing the beneficial potential such technologies can harbor.

An important lesson is that technology itself is neither good nor evil, but can amplify good and evil if adequate processes and norms are not in place. Regulation should therefore invariably focus on the use and outcomes of technologies, and not limit or prohibit the technologies themselves. Any powerful technology can be abused or be used for the betterment of humanity. The solution to technology-related problems are often more technology; technology is needed to grow the renewable energy sectors to fight climate change, biotechnology is necessary to raise crop yields and cure illnesses. We should not revert to a naive utopian era of IT as savior, but should instead critically examine the impact of new technology to help maximize its value and limit harms

Going forward, policymakers should understand that most people see technology as an essential and valuable part of their lives, and that they seek and desire new innovations and improvements—but that where there are challenges and issues, government acts in a limited and responsible manner to deal with the problems at hand in a manner which cause the least possible harm to competitiveness, innovation, or consumer welfare.

Industry stands ready to work with governments everywhere. Last year, Facebook CEO Mark Zuckerberg encouraged a broader debate on how to update the rules of the Internet globally in four areas: harmful content, election integrity, privacy and data portability[19]. Microsoft CEO Satya Nadella in January urged lawmakers, industry and other stakeholders to reach a consensus on how best to address law enforcement data access and encryption concerns taking into account the equally important privacy and security considerations.[20] Microsoft CEO Brad Smith has encouraged industry to work with lawmakers to develop rules to limit the use of controversial facial recognition technologies[21]. Apple CEO Tim Cook has previously called for stronger laws protecting individuals' access and rights to their personal data on the Internet. Alphabet CEO Sundar Pichai in January urged governments to work with industry in setting up a regulatory framework for artificial intelligence in order to address the potential negative consequences of AI, including deepfakes and facial recognition[22].

At the 2020 World Economic Forum in Davos, IBM CEO Ginni Rometty announced its new Policy Lab, "a new forum providing policymakers with a vision and actionable recommendations to harness the benefits of innovation while ensuring trust in a world being reshaped by data"[23]. The Lab intends to offer "precision regulation" to help foster trust and transparency in artificial intelligence.

The anxiety and doubts surrounding technologies can best be alleviated by broad, multistakeholder debate about the global rules we need to clearly define the responsibilities for people, governments and industry as we enter the Fourth Industrial Revolution. As history has shown us, technology has aided humanity in curbing such ills as infant mortality, hunger and ignorance. Despite the many challenges facing the human race, from global warming, hunger and food security, economic growth and social inclusion, and the future of the Internet, the solution to such problems calls for the careful deployment of more technology, not less. We must all work together to achieve the promise of the digital age for all.

## About WITSA

WITSA is a global consortium of leading ICT industry association members from over 80 countries/economies. WITSA members represents over 90% of the ICT industry.

As the leading recognized voice of the global ICT industry, WITSA aims to drive transformation and expand the use of ICT globally; given that ICT is the key driver of the global economy.

WITSA's members and stakeholders comprise national associations, multinational corporations, institutions and organizations, researchers, developers, manufacturers, software developers, telecommunication companies, suppliers, trainers and integrators of ICT goods and services. As such, they represent a large and obviously vital constituent group for whom the effective balancing of concerns and rights affecting the security, privacy and information capability provided by ICT products and services underpins business development and economic activity.

---

[19] https://www.washingtonpost.com/opinions/mark-zuckerberg-the-internet-needs-new-rules-lets-start-in-these-four-areas/2019/03/29/9e6f0504-521a-11e9-a3f7-78b7525a8d5f_story.html

[20] https://www.wsj.com/articles/tech-giants-new-appeal-to-governments-please-regulate-us-11580126502

[21] https://www.washingtonpost.com/news/powerpost/paloma/the-technology-202/2018/12/07/the-technology-202-microsoft-s-brad-smith-says-other-tech-companies-need-to-get-behind-a-facial-recognition-law-too/5c095c1f1b326b60d128014e/

[22] https://www.washingtonpost.com/news/powerpost/paloma/the-technology-202/2020/01/21/the-technology-202-google-s-sundar-pichai-is-the-latest-tech-titan-to-embrace-regulation/5e25fbf1602ff14e66055e11/

[23] https://www.ibm.com/blogs/policy/ai-precision-regulation/

WITSA is a founding partner of the Digital Trade Network (DTN), a new initiative providing a permanent private sector resource for digital trade policy makers in Geneva. Through DTN, WITSA works with a number of other partner organizations to build an impartial, broad base of international supporters to work with the WTO, the UN Conference for Trade and Development (UNCTAD), the International Trade Centre (ITC), and related economic policy agencies in Geneva with a focus on the networked economy.