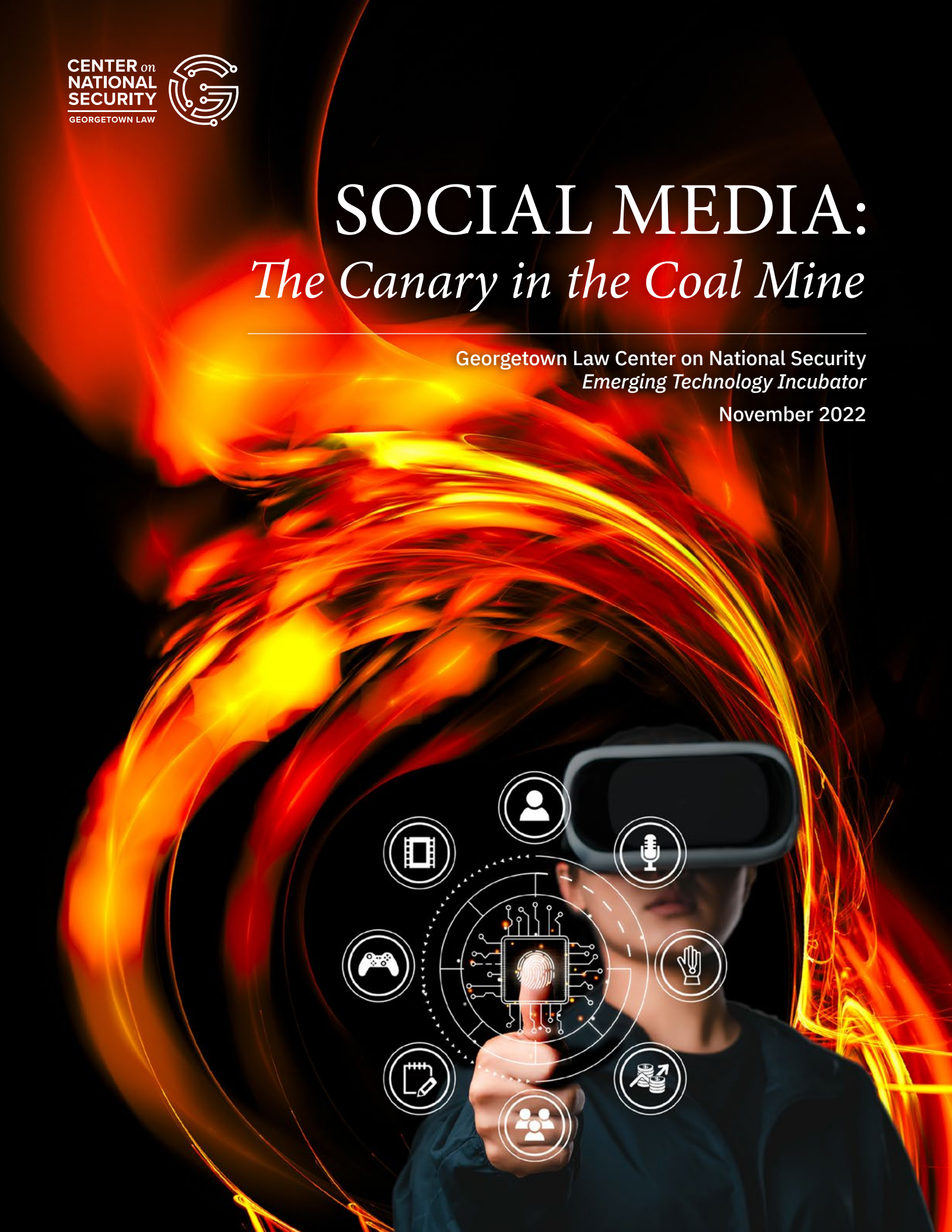
CENTER *on* NATIONAL SECURITY
GEORGETOWN LAW

SOCIAL MEDIA:
The Canary in the Coal Mine

Georgetown Law Center on National Security
Emerging Technology Incubator

November 2022



SOCIAL MEDIA:
The Canary in the Coal Mine

A Digital Bill of Rights,
Developers' Code of Conduct, and
Information Governance Principles
for a Healthier Digital World

Laura K. Donohue, Principal Investigator

Georgetown Law Center on National Security
Emerging Technology Icubator

NOVEMBER 2022

Supported, in part, by a grant from the Open Society Foundations

TABLE OF CONTENTS

I. Executive Summary

The internet and social media are experiencing transformational growth, creating massive opportunities alongside unprecedented, novel national security threats. On the one hand, social media offers an unprecedented opportunity to connect with others half a world away, to create communities and shared experiences and to allow for tremendous growth in knowledge and understanding. On the other, social media and new internet technologies field accusations that they are weaponized to catalyze genocide, evade global sanctions, launder money for terror groups, radicalize violent extremists, surreptitiously track politicians, and undermine democracies worldwide, among other national security concerns. This report offers a Roadmap for a Healthy Digital World (Roadmap), a comprehensive strategy identifying practical steps to address emerging threats while fostering the evolution of this increasingly important global ecosystem.

The report first provides a short background on "social media" itself — a term that includes online digital platforms, websites, services, and apps built around user-specific profiles that openly create, share, and exchange user-generated content.[1] Such content is shared in digital public spaces, which may take different forms: a user's feed, a website homepage, or the digitally rendered landscape of a videogame. Increasingly then, almost all internet activity occurs in the context of some form of "social media" interaction, whether users are watching a Youtube influencer for financial advice, chatting with new friends in Discord channels, or even review-bombing a restaurant on Yelp. As social media swallows more of our daily interactions, there are a few primary technologies likely to shape the future of the internet: artificial intelligence, extended realities, cyber infrastructure, Web3, and biodata collection. The report briefly explains each, and how they contribute to a future, interconnected ecosystem. Understanding the complexity of this networked growth, rather than any technology in isolation, is key to anticipating major national security threats likely to evolve.

From this understanding of the future of social media, the Task Force zeroed in on six critical, emerging threats: lowered barriers for bad actors; information chaos; psychosocial and physical harm; loss of innovation; exploitation of power; and negative externalities. Similar to the technologies, the threats are interconnected and can come into tension. For example, slowing the deployment of technologies in favor of added cybersecurity could prevent physical or psychosocial harms. However, such slowing could doom American companies in the race to market, giving first mover advantage to less responsible actors who reap the major financial benefits. Over time, such losses hurt the research budgets of American companies and undermine American private sector innovation, a key driver of our national security and economic prowess. The harms identified extend across our on and offline lives, with different repercussions in each.

Although law enforcement focuses on offline harms, as virtual life expands to encompass more human activity, such distinctions will blur. The online world has proven fatal to some social norms that underpin our safety and our democratic society. Online threats increasingly implicate the physical world, and the American national security apparatus isn't prepared for the enormity of this transition.

To address these threats, the report offers the comprehensive Roadmap for a Healthy Digital World that focuses on reinforcing effective governance, responsible platforms, and an empowered public, with specific pathways to achieve each. It details vital democratic principles to protect, potential actors and actions available in this space, criteria for evaluating potential solutions, as well as concrete recommendations, culled from the collective wisdom of a diverse, high-level Task Force convened by the Georgetown Law Center on National Security. Furthermore, the Roadmap proposes a draft Digital Bill of Rights to empower the public; a Developer's Code of Conduct to hold technology and companies to a higher standard; and Information Governance Principles, to prioritize policy making in this arena.

The Roadmap developed from a yearlong deep dive undertaken by the Georgetown Center for National Security, with guidance and recommendations endorsed by the aforementioned Task Force. The Task Force included technologists, computer scientists, venture capitalists, constitutional law scholars, members of Congress, federal judges, privacy advocates, government regulators, rural and civil rights activists, student journalists, federal prosecutors, and other experts from diverse backgrounds.* Their deliberations benefited from a Research Consortium of experts and approximately 100 stakeholder interviews, which extended across urban/rural, political, ethnic and racial, gender, age, geographic, disability, and socioeconomic lines. From social media influencers to consumer advocates, we have tried to make space for all who have a stake to be heard.

The message is clear — social media is the canary in the coal mine for the wider internet. As emerging technologies alter and expand our daily interactions with the virtual world, the concerns they raise will magnify exponentially. The future of our national security, as well as the basic functioning of democratic governance, are at stake. We hope this Roadmap provides a foundation for future policy and planning efforts to foster the growth of the internet and social media in ways that strengthen national security and democracy.

Roadmap to a Healthy Digital World

To address these threats, the Roadmap serves as a long term guide for decision making. It begins with conceptual frameworks that can be adapted as technology and the societal climate evolve. A list of core democratic principles, actors for change, and criteria for optimal solutions memorialize the values and practicalities that solutions will need to take into account. Rather than being exhaustive, they are meant as guideposts for future efforts, to reduce the need to "reinvent the wheel" under rapidly changing circumstances. To start, the Roadmap identifies ten principles that would most contribute to maintaining and fostering a healthy democracy. It next enumerates the actors with technical expertise and power likely to play key roles in the near future, enabling any public servant or private sector leader to identify leverage points for change. The Roadmap also offers criteria for evaluating policy proposals, with an emphasis on principles that could be adapted beyond the social media space. These are the same criteria used to evaluate and recommend the solutions endorsed by the Task Force. Each of the abbreviated lists here are expanded upon in the body of the report.

**All members of the Task Force have participated entirely in their personal capacities and not on behalf of any other organization or entity. The recommendations put forward are not attributable to any individual members. Not all members work directly on, or profess expertise in, all of the recommendations set forth below; nevertheless, this set of recommendations reflects the sense of the Task Force as a whole.*

DEMOCRATIC PRINCIPLES TO PRESERVE

MAJOR ACTORS FOR CHANGE IN SOCIAL MEDIA AND THE INTERNET* **abbreviated from the comprehensive list provided in the body of the report*		
GOVERNMENT	**PRIVATE SECTOR**	**CIVIL SOCIETY**
Department of Defense	Internet Platforms	Journalists and Media Organizations
Department of Justice and FBI	Telecommunications Companies	Libraries, Museums, and Other Civic Education Groups
State Department	Technology Startups	Consumers
Federal Trade Commission	Financiers	Foundations
Federal Communications Commission	Influencers	Professional Organizations and Chambers of Commerce

CRITERIA FOR EFFECTIVE SOLUTIONS TO BUILD A HEALTHY DIGITAL WORLD

Following the macro strategy, the Roadmap delves into more concrete recommendations organized by the three primary categories of actors for change—government, internet platforms, and the public. The Task Force endorsed three guiding recommendations as first steps towards a healthier digital future, and developed a list of ideas for their implementation. The compendium of these further ideas to implement the recommendations draws upon the Task Force's collective expertise. They cover myriad actors in society, reinforcing the need for creative collaborations to protect U.S. national security and democratic governance.

TO ACHIEVE:	
1. Effective Governance	Policymakers should identify and codify protections against harms that apply to the digital world, and provide funds for research and grant programs for investigating and responding to those challenges.
	POTENTIAL STEPS TO ENACTMENT: • Federal research consortium examining emergent online harms • FTC clarifications on platform data sharing with researchers • Grants to explore responsible information governance practices • Exploration of disclosure and reporting requirements for platforms to help understand where reform is most pressing
2. Responsible Platforms	Industry, civil society, academia, and the public should develop a users' Digital Bill of Rights and a Developers' Code of Conduct and promote their adoption and adherence.
	POTENTIAL STEPS TO ENACTMENT: • Formal commitments by platforms and other tech companies to a Digital Bill of Rights and Developers' Code of Conduct • Interagency working group with formal channels for public input and education • Self-regulatory industry collaborations around Information Governance Standards • Support for diverse employee perspectives and inclusion work, particularly in content moderation and community safety • Company training to facilitate employee conversations and action around digital rights and ethics
3. Empowered Public	All stakeholders, including government, platforms, community groups, academia, and civil society, have an obligation to educate and provide tools to online users so they are empowered to think critically, to advocate for their interests in the digital world, and to participate in democratic processes.
	POTENTIAL STEPS TO ENACTMENT: • Locally-focused, content-neutral civic education for K-12 students and adults • Support for local arts, culture, and journalism to build communal cohesion and a common local base of factual understanding • In-person community conversations to set online norms, reinforce civil online interactions, and create new outlets for online dispute resolution outside the platforms themselves • Workshops and influencer outreach campaigns to reach new audiences and build coalitions • Grassroots campaigns to catalyze the adoption of new user tools, platform policies, and regulatory frameworks • Interoperability standards giving users more control over their profiles, content creation, and personal data • User interface adjustments, like a button to easily communicate a user's personal level of assuredness about the credibility of the content they share

IMPLEMENTATION TOOLS

The Task Force developed initial versions of three of the documents referenced in the recommendations. The Digital Bill of Rights provides ways to preserve democratic principles in the future online world. The Developers' Code of Conduct, modeled on the Hippocratic Oath and Bar oaths for lawyers, highlights ethical values and seeks to establish a cohesive sense of professional conduct in a career that is relatively unregulated compared to other professions with similar power over the future of society (e.g., scientists, lawyers, investment advisors, or mechanical engineers). The Information Governance Principles form the basis for ethical principles in the investing world, guidance for government policymakers, and standards for industry self-regulation among technologists and entrepreneurs. Abbreviated here, the full documents in the body of the report provide a jumping off point for future debates.

Sample Digital Bill of Rights

i. Individual Rights
- Right to Identity
- Right to Bodily Autonomy & Integrity
- Right to Control Data, including:
  - *Data Transparency*
  - *Biometric Data*
  - *Data Portability*
  - *Data Security*
  - *Express Consent*

ii. Rights within the Public Square
- Right to Free Association
- Right to Verification
- Right to Block
- Right to Due Process/Right Against Erasure
- Right to the Physical World

iii. Participatory Rights
- Right to Inclusion in Decision Making
- Right Against Discrimination
- Right to Protection of Vulnerable People/Communities
- Right to Accessibility
- Right to Communal Safety

iv. Algorithmic Inclusion and Transparency
- Right to Algorithmic Transparency
- Right to Financial & Business Model Transparency
- Right to Representation

v. Tools to Navigate the Public Square Safely
- Right to Digital Public Education
- Right to Disconnect
- Right to Notification
- Right to be Free from Deceptive Commerce

vi. RIGHT TO ENFORCEMENT
- Right to Enforcement Information

Draft Developers' Code of Conduct

- ☐ I pledge to design projects with public safety, human rights, democracy, and the good of society in mind.
- ☐ I pledge to refrain from intentionally causing harm to my enterprise, society, or others, in service of my own personal gain.
- ☐ I pledge to make the fruits of my efforts accessible to all people, regardless of race, sex, disability, or other status.
- ☐ I pledge to architect my products to provide data and functionality through publicly available and documented APIs and service interface calls that will be externalizable.
- ☐ I pledge to develop products who's user experience provides less friction and better ease of use in every iteration.
- ☐ When confronting a problem with uncertain impacts, I will seek input from others, including those who might face disproportionate impact, and consider the risks before proceeding and throughout.
- ☐ I will respect the privacy and sanctity of individuals, taking care to ensure the security of their personal data and only using it with their approval.
- ☐ I will aim for transparency and share my knowledge as much as possible, to help advance scientific knowledge and to open that information to all who come after me.
- ☐ Most importantly, I will remember that technological innovation is meant to serve the good of humanity, and I will strive to contribute to that progress.

Information Governance Principles

1. Information Integrity
2. Democratic Norms
3. Intellectual Diversity
4. Privacy
5. Universal Accessibility
6. Special Protections
7. Data Ownership
8. Openness
9. Fairness
10. Accountability

II. Introduction

Our world is changing, fast. Competition among the "great powers" is no longer measured by one dimension, as nations vie for dominance in the arenas of commerce, innovation, infrastructure, and more. Further complicating this picture is the expanding impact of non-state actors on national security concerns. Major corporations invest billions in technologies previously of interest mostly to government research. Scammers spoof esteemed military generals on dating websites. Terrorist organizations radicalize new recruits through social media channels. In this increasingly complex world, new tools must be adopted to bolster conventional instruments of power like defense and diplomacy. Social media is the canary in the coal mine for the paradigm-shifting changes to come, as new technologies spread quickly across society before the national security community can effectively protect against their weaponization. This Report offers a comprehensive strategy to meet these challenges, what we term the Roadmap to a Healthy Digital World (Roadmap). We encourage you to turn directly to the Roadmap, and to use the rest of the report as important context to enhance your understanding of the issues the roadmap seeks to address.

Initially, the idea of social media as a major national security threat was almost unthinkable. A tool used to rate attractiveness, connect old classmates, or share recipes, in its early stages, did not strike a particularly concerning profile. Yet as it became more established, the picture became more complicated. Social media became an organizing tool for violent extremists, the primary conduit for misinformation and propaganda, a major surveillance and targeting device, and a key driver in efforts by our adversaries to undermine American democracy. Hundreds of social media studies focus on disinformation/misinformation and the 2016 and/or 2020 elections, with good reason.[2]

Despite the allegations against social media, it remains a phenomenally useful, entertaining, and connecting force for good in the lives of many. It has become a societal juggernaut, rapidly transforming the way individuals communicate, learn, play, shop, invest, and more. Balancing these complex realities outside of spaces that would normally be considered the purview of national security presents a challenge. Social media is the quintessential modern security threat, fundamentally rewriting our societal interactions in positive ways, while expanding so rapidly that it leaves us vulnerable to significant, perhaps even existential, dangers. We can't — and shouldn't — stop social media, but we can blunt its worst harms.

This Report is a first attempt at anticipating the **future** threats catalyzed by the evolving landscape. We assembled a diverse Task Force to identify key technologies, to catalogue the most concerning risks, to establish the principles most critical to protect for a healthy internet ecosystem, and to offer comprehensive recommendations for the path forward.

We distill that work into three parts. First, we offer an assessment of the current state of social media and the internet, including their tangible benefits for all of society. Second, we outline the major harms or threats of the current social media landscape that we expect to magnify over time. Third, we detail the Task Force's recommendations to address the most significant of the challenges previously identified, including a framework to guide future problem-solving efforts, concrete steps for today, and tools to assist with their implementation.

At its core, this Report is our attempt to draw attention to a new class of national security challenges, where the security threats blur into the fabric of daily life. Social media is the canary in the coal mine in two senses: it is both a warning about the rapidly transforming future of the internet, and the rapidly transforming future of national security itself.

III. Understanding Social Media

A. Defining Social Media

Social media itself is an amorphous term, particularly as new platforms blend traditional media, cash transfers, gaming, physical sales, video calls, restaurant reviews, and more into endless combinations for users. Much as our phones have become our cameras and alarm clocks, our social media platforms are gobbling up our online presences, as well as aspects of our physical presences. For our purposes then, social media includes online digital platforms, websites, services, and apps built around user-specific profiles that openly create, share, and exchange user-generated content.[3] An essential component of this definition is that social media allows users to interact on digitally "open" or "public" platforms. Platforms often go beyond the private one-to-one communication of email or text messages by making user-generated content shareable and accessible to networks or groups of users. Digital public spaces may take different forms: a user's feed, homepage, or the digitally rendered landscape of a videogame and shared content often travels across user networks according to algorithms.[4] Anonymous, pseudonymous, or fully identified users can interact with one another and exchange information to connect, network, play games, trade, or learn.[5] Open exchange of content allows platform users to easily form large online communities around any common interest, idea, or motivation.[6]

Whether it's the traditional Facebook group, sub-Reddit forums, or a dedicated YouTube subscriber base, social media promotes the formation of online groups in a way not possible in the pre-internet era. Because of the nature of online interaction — the ability instantly to share information regardless of geographic distances — these groups can maintain millions of members who engage regularly and impactfully with one another.[7] The fact that social media platforms are not device-specific but operate across computers, mobile devices, and gaming consoles and that such devices are near-ubiquitous means that barriers to entering online communities are extremely low.[8] Social media participation has grown substantially, and in meeting that demand, platforms have evolved to touch every aspect of a modern user's life.

While nascent forms of social media such as Friendster, Myspace, Facebook (now Meta), and Twitter focused directly on the "social" aspect of social media — connecting users online for the sake of forming social or friend groups — modern social media is more ambitious in its reach. TikTok, Truth Social, 8Chan, Discord, Clubhouse, Whatsapp/Telegram groups, and others offer users much wider choice in their social engagement. Platforms like LinkedIn have become integral to professional advancement, while those like Microsoft Teams and Slack are mainstays of the modern workplace, allowing employees to efficiently share work products, manage projects, and communicate through group chats and video-interfacing.[9] Additionally, modern social media platforms have found a foothold in financial services; "Finance TikToks"

or "FinToks" wherein influencers relay financial advice to users are increasingly popular[10] social trading networks like E-Toro allow Twitter-like commentary on financial products and investments,[11] and parts of the cryptocurrency ecosystem are being integrated in wide-reaching multi-player online gaming platforms, thus blurring the lines between social media, gaming, and investing.[12]

The breakneck advance of social media is far from complete. The Covid-19 pandemic has breathed new life into platform expansion.[13] In the last few years, providers have made concerted efforts toward building the Metaverse: an all-encompassing virtual world aimed at integrating one's social, professional, and financial online presence into one or multiple immersive platforms.[14] This developmental trend toward the Metaverse (or multiple metaverses), along with the emerging technologies deployed to attract and immerse its users, has profound implications for how users engage with technology, each other, and the data they generate.[15]

CURRENT MAJOR PLATFORMS

In the current social media and internet landscape, the major platforms include Alphabet, Meta, Microsoft, Apple, and Amazon. In 2021 these companies alone spent $149 billion on research and development (R&D), equivalent to roughly a quarter of the total R&D spent across private sector and significantly higher than the largest government R&D budget, that of the Pentagon.[16] An estimated 5%–20% of this R&D is spent on cutting edge technology, which includes the metaverse, autonomous vehicles, AI, robotics, fintech, crypto and quantum computing.[17] Other technology players are also entering the arena, as giants like Oracle route TikTok's US traffic and Salesforce acquired Slack. While these companies are spending heavily on R&D and finding new synergies, expert views split over the extent of market competition and its effects on innovation and overall industry development.

On one hand, the major platforms possess significant market share in their respective industries and are able to keep would-be competitors out by keeping start-up barriers high and engaging in "killer acquisitions."[18] Social media companies depend on network effects, which discourage interoperability and encourage acquisition of competitive technology. This approach is not without its challenges. The FTC, for instance, filed complaints against Facebook (now Meta) for its acquisition of its competitor WhatsApp and Google for its acquisition of Waze, a popular GPS navigation app.[19] A House Judiciary subcommittee Report on antitrust among technology companies found that such acquisitions create big technology monopolies which "materially weakened innovation" and hurt consumers.[20]

On the other hand, there is some evidence that large technology companies engage in fierce competition with one another. Meta and Microsoft are currently competing to create immersive experiences by creating metaverses on their native ecosystems. Microsoft is trying to expand its metaverse technology through expansion of its gaming platforms, evinced by its near $70 billion acquisition of Blizzard-Activision. Similarly, Meta has invested over $10 billion in acquiring and developing the software and hardware necessary to innovate in XR. To support that investment, Meta has launched an innovative AI supercomputer which will assist in developing real-time voice translation software to be employed in the metaverse to identify harmful and prohibited content on its platform. Apple competes with Google and Meta by prioritizing user privacy over data monetization. To the extent that large technology companies recognize and compete on privacy, consumers are arguably made better off.

Technology is a notoriously volatile field, and the Goliaths of today may continue to reign or could be toppled by new disruptors. This description therefore represents a snapshot in time, one that may inform future discussions about the prominence, power, and activities of future tech giants.

BENEFITS OF SOCIAL MEDIA

The Task Force sought to recognize and preserve, to the greatest extent possible, the immense benefits of social media, such as efficient sharing of information, the construction of more and stronger relationships, and cultural exchange. Social media can and has amplified users' voices concerning corporate social responsibility, political grievances, and personal experiences. Before focusing on harms, here is a brief summation of some of those material benefits, so as not to lose sight of the incredibly valuable elements worth preserving and helping to flourish.

Social media platforms have substantially increased the speed with which individuals can share information. They provide more sources of information and more efficient mechanisms for sharing that information than traditional media outlets. Indeed, social media users have often been the first to Report ground-breaking news events such as the Ebola Outbreak, Paris Terrorist Attacks, or mass shootings.[21] Consequently, most users regularly turn to social media for their news.[22] This may be partly because these platforms share information quickly by bringing a panoply of information across users' feeds.[23] But users share more than just news — every day, billions of users log on to share information about everything from family recipes to political ideas to warnings of local crimes.[24] Governments and public institutions use it to inform citizens about health and government services.[25] The increased speed with which information is generated and disbursed is a virtue to the extent that more people can access pertinent and helpful information.

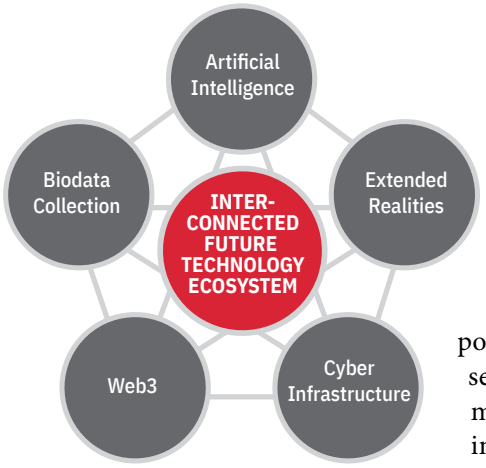
At the heart of social media is increased connections. About two-thirds of users turn to social media to stay in touch with family, current friends, and to reconnect with old ones.[26] Immigrants turn to social media to maintain social and cultural ties with their home country. These connections have been linked to increased self-esteem, perceived support, and decreased loneliness among users.[27] Social media connections, however, are hardly confined to maintaining in-person relationships. Instead, the borderless nature of social media makes it easy for users to connect with a diverse set of individuals across the globe. Unless censured, user content flows from its origin across the platform based on algorithmic variables irrespective of geography. Consequently, it's not uncommon for popular trends in one country to move across a given platform, propelled by engagement from foreign users. Users in some cases are more likely to interact regularly with people from different political parties, income levels, and racial or ethnic backgrounds than they would be without access to the medium.[28]

Social media empowers users to be heard and make their content impactful. It allows consumers to engage with corporations, citizens to organize and effect political demonstrations, and historically marginalized users to amplify their experiences. Social media provides a medium for consumers to communicate with corporations and actively shape discussions surrounding corporate social responsibility.[29] By responding to specific policies or concerted marketing campaigns, consumers communicate what is important to them and, as a result, lead corporations to make substantial changes in the way they engage with the public and the initiatives they undertake.[30] The platform has proved to be a useful tool for citizens to communicate, discuss, and act on political grievances. Users have facilitated civic protests internationally; countries ranging from Spain to the Philippines and Hong Kong have all seen mass political demonstrations ignited by social media.[31] The newfound speed with which citizens can air grievances against their government and organize has restored some political power and influence to disenfranchised citizen populations.

The same features of social media that facilitate consumer influence and political participation allow historically marginalized communities to amplify their voices. Increasingly, historically discriminated against minorities turn to social media to Report instances of discrimination and share their experiences online.[32] Users can better cope with and combat racial, ethnic, sexual, or cultural discrimination by rely-

ing on social media to raise awareness and for social support.[33] Additionally, on a group level, minority groups can expand the reach of their cultural and religious influence and mitigate adverse cultural perceptions through social media.[34] Together, these practices empower minority group members to better advocate on their behalf and mitigate negative cultural perceptions.

In short, social media has opened the channels of user-oriented communication. Its benefits extend beyond those enumerated here; however, they do not come without cost. Many of the same reasons that make social media useful to users raise concerns related to cybersecurity, data privacy, and national security.



B. Relevant Emerging Technologies

Five major categories of technologies likely to play a key role in shaping the future of the internet include extended realities, artificial intelligence, Web3, biodata collection, and cyber infrastructure. They represent some of the highest concentration of research funds and focus in industry, and based on unclassified sources, in government. While each holds much promise to improve American lives, each also poses unique challenges and national security concerns. This section describes each technology, its current state of development, and potential future capabilities, to provide background information for the wider concerns raised in this Report.

EXTENDED REALITIES

Extended Reality (XR) technology is focused on furthering the quality and scope of human-computer interactions by integrating virtual and physical worlds. It is an umbrella term for technology that includes virtual, augmented, and mixed reality. Though there exists significant overlap, each subset of technology varies in its level of integration with the physical world and as a consequence, its applications. Virtual Reality (VR) often involves a headset which creates an immersive audio-visual experience by taking users to a completely virtual setting.[35] VR comes with various attachments and devices worn on the body (wearables), such as controllers or haptics that incorporate tactile feedback to users. Augmented Reality (AR) may employ headsets but also utilizes cameras to superimpose digitally rendered images onto real-world physical backdrops.[36] Mixed Reality (MR) goes a step further by focusing on allowing digital elements to be manipulated, such as typing on a projected keyboard.[37] These categories represent a continuum of evolving technology that is increasingly blurring distinctions between human experiences in physical and virtual settings.

The integration of physical and virtual worlds, however, generates an ever-growing amount of data. A sophisticated VR system might generate and track reams of geolocational, biometric, and motion-oriented data to sync audio-visual and tactile feedback with user interactions.[38] Similarly, AR and MR devices use lidar technology to map out physical surroundings and create virtual representations.[39] To the extent that these systems are integrated with other personal information (names, login credentials, financial statement balances, physical characteristics of Avatars, audio-visual recordings), XR systems might store an encyclopedic rendering of the most intimate details of an individual's life.

Increased data generation is of particular concern since XR technology is finding many new applications across industries. XR technology is increasingly used in gaming, education, consumer devices, manufacturing, engineering and design, and professional and military training programs.[40] While many of these

applications might allow sophisticated parties to have meaningful control over the data generated by the XR they employ, consumers are increasingly at risk of giving up control over their data. For example, popular games like PokemonGo, a VR based smartphone application or Nintendo's VR Mario Kart Live create reams of personally identifying data that is stored in-app.[41] The latter requires users to create a detailed virtual map of their homes to create a home-oriented racetrack.[42] AR filters on Instagram, Snapchat, and other social media apps create and collect data about facial geometry. Most recently, Meta faced a class-action seeking an injunction on the use of specific AR filters on Instagram and Facebook.[43]

While XR data collection stokes privacy concerns, the technology also can directly threaten individual autonomy. In Beijing, Chinese law enforcement has rolled out a beta program, for instance, that uses AR-based facial recognition sunglasses to identify individuals in crowds.[44] The sunglasses use facial recognition technology to match individuals against an offline database. Researchers at the University of New Haven exposed XR technology's vulnerability to malware that would allow attackers to change VR representations for headset users.[45]

XR technology is rapidly developing. In 2021, it was valued at about 31 billion.[46] It is forecasted to be closer to 300 billion in 2024.[47] The US is the leader in patents filed for XR, with Japan a close second, Korea third, and China a distant fourth.[48] Recently, there has been an increase in academic research on Brain-Computer Interface (BCI) technology. In one study, researchers were able to translate brain activity to allow users who imagined manipulating an AR represented cube.[49] Another study translated brain signals into speech.[50] Soon after the latter research, Meta issued a statement describing how breakthroughs in BCI are likely to pave the way for more integrated and immersive VR and AR experiences.[51] Despite these improvements in XR technology and in light of the Covid-19 pandemic, the public is still reluctant to see it as a helpful application beyond gaming.[52] Extended reality technologies have a long way to go, but their promise is drawing immense interest from industry behemoths that merits further examination.

ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

Artificial intelligence (AI) systems allow machines to act based on data collected from the environments around them, typically relying on machine learning (ML).[53] ML is a subset of AI algorithms where the underlying algorithm is changed generationally based on outputs from a feedback loop.[54] For example, the operation of deep learning (also known as deep neural networks (DNNs), one of the breakthrough MLs that has contributed most to AI in the past decade, is based on communication neural networks within the human brain and can process a large quantity of data to classify images, recognize speech, and take on other roles.[55] AI is the "nut" of social media networks, facilitating the algorithmic categorization, classifications, and predictions via which we are all segmented and micro-targeted through business models. News feeds, "like/dislike" buttons, and automated content presentation as on TikTok, are all powered by artificial intelligence according to the values and parameters of each social media company. To introduce our national security parlance, algorithms are the social media equivalent of the Gatling gun, an early machine gun that arguably revolutionized war-fighting.

AI is already revolutionizing the ability of internet companies to target individuals with personalized news and advertisements, deanonymize large data sets, and find patterns across huge volumes of user behavior. A potential weakness of AI/ML remains the ability to poison data used to create algorithms: hostile parties can feed the AI/ML specially crafted images that train the system incorrectly and cause misidentification of an entire series of items.[56] These poison images are sometimes harvested from social media platforms.[57] Beyond intentional poisoning, unconscious bias in the development of algorithms, by the people writing the algorithms or coding results to train them, is a massive issue for which there are no good answers currently.[58] In addition, many language processing algorithms are initially trained on data sets of all online

materials or books in the English language, a data set that skews heavily white and male, before an algorithm's particular task is even assigned.[59] In addition to broader quality concerns, non-standardization and balkanization of data systems limits usable data sets and potentially introduces more points for bias, limiting the ability to successfully train algorithms. In this way, authoritarian regimes like China have a major advantage, as government collected databases unhindered by privacy rights can be shared across chosen government-connected companies, improving their algorithmic learning over what is possible in an America promoting private sector competition and more concentrated on individual rights.[60]

AI/ML also presents interesting questions for the arts and content industries. Programs like DALL-E from OpenAI create art using algorithms that crunch publicly available artistic images into mimics of certain artistic styles that range from creepy to award-winning.[61] OpenAI has a similar program for natural language processing that produces similarly mixed yet promising results.[62] Such technologies highlight loopholes in our intellectual property laws and raise questions about what it means to "copy" an artist's work when that work is the basis, in part, for an algorithm's production of a new work. They also raise concerns around continued incentives for innovation and creativity in certain industries, the ease of scamming or counterfeiting art, and other potential uses for elaborate, unlimited content creation in user manipulation. Deepfakes highlight the possibilities for this last concern. Deepfakes are realistic photos or videos of a fake event created through media manipulation.[63] Deepfakes pose a threat to consumers who lack the ability to verify the veracity of information, thereby representing a serious potential for misinformation circulated through social media.[64] Still, most of the greatest fears about deepfake technology have not come to pass, and some experts are skeptical that deepfakes will become advanced enough to wreak the large-scale havoc feared. With new art generation technologies, deepfakes, and the myriad other applications of AI/ML, we are hurtling towards a future internet rife with opportunities for compromises of national security and societal stability.

WEB3

Web3 is an umbrella term we use here to include cryptocurrencies, nonfungible tokens (NFTs), decentralized autonomous organizations (DAOs), decentralized finance (DeFi), decentralized exchanges (DEXs), decentralized applications (dApps), and other potential applications of blockchain and other technologies that offer new methods of transacting and organizing society. Blockchain is a distributed ledger that can store data. Through identical copy distribution across databases of entire networks, blockchain becomes exceptionally difficult to hack or cheat, providing substantial user protections.[65] With every set of new data that is added to the network, a new "block" attaches to the "chain".[66]

Currently, blockchain is best known as the basis for cryptocurrencies.[67] Cryptocurrencies are online versions of money that store value generated by online interest communities via blockchain networks. Cryptocurrencies, like paper money, have value because a community of people is willing to trade them for goods or services, imbuing a currency like Bitcoin a status its supporters call akin to digital gold.[68] Continuing the analogy to gold, cryptocurrencies like Bitcoin and Ethereum are increasingly renowned as a volatile but possibly lucrative new investment class, offering utility beyond investing in government-backed paper currencies that are not considered to offer the same possible returns.[69] That being said, a number of countries including the United States are considering the introduction of their own central bank digital currencies, which would marry the convenience of crypto with government-backing to reduce volatility of value.[70] Besides cryptocurrencies, blockchain is best suited to any transaction that requires an instantaneous, trust-less environment.

NFTs are one such additional application. NFTs are unique entries on a blockchain ledger that correspond to digital or physical assets. Those entries are simply data or metadata for existing file formats like JPEGs,

EXIFs, PDFs, or others. In this way, they can prove ownership of original artwork, track raw materials across a supply chain for major companies, or authenticate limited edition luxury goods for customers. NFTs differ from cryptocurrencies because unlike digital currencies, which are fungible tokens, NFTs are not identically interchangeable. In the social media realm, NFTs and cryptocurrencies both have accumulated financial value based on emerging concepts of digital-world value and ownership. For example, an NFT can prove ownership of a digitally created image, even when millions of free copies of the original image are easily made. Due to the speculative nature of both NFTs and cryptocurrencies, they are common targets of, or fronts for, "pump-and-dump" schemes and other financial manipulation. Ironically, due to the digital and communal nature of these assets, many of these frauds are perpetrated using social media influencers and communities to lure victims or otherwise convince individuals to invest far beyond their means.[71]

DAOs are collectives of individuals via a blockchain system that allows them to vote within a community, raise money for projects, and even pay individuals for DAO upkeep or work products outside of the blockchain network. To communicate, DAO members often organize on various social media sites like Discord or through other chat functions, using internet platforms to facilitate community cohesion, lobby for different voting initiatives, and coordinate large off-chain projects. DAOs operate without a centralized government, they are controlled through rules that are encoded into transparent computer programs that are in turn controlled by the members of the organization.[72] As a result, by embedding the rules into code, there is no need for managers and hierarchical structures.[73] This structure means that remedies for legal issues arising from DAOs are limited, as DAOs blur individual responsibility. In response to these concerns, states like Wyoming are creating LLC structures to incorporate DAOs, but the efficacy of these accountability mechanisms remains untested.[74] In this way, DAOs may represent the future of social media-facilitated social organization, for better and worse.

DeFi is a new frontier in finance, including cryptocurrencies, that seeks to use blockchain systems to bring trust-less automation to a variety of financial transactions. DEXs are a key player in the DeFi ecosystem, as parallels of financial exchanges like the New York Stock Exchange that allow for instantaneous trading at any hour of the day. dApps are parallels to other existing applications, from social media to gaming, built on the same decentralized principles and technology as blockchain networks.

Other uses of blockchain include to create carbon offset marketplaces, support secure voting systems, and distribute government benefits payments like social security or welfare. In one striking example, the Kiva Identity Protocol, built on Hyperledger, offers Africa's first national decentralized identity system, enabling Know Your Customer protocols to help the unbanked access capital.[75] Estonia has migrated significant portions of its government activities online using blockchain technologies, and 99% of public services are available to citizens as e-services.[76]

However, not all of these uses are ready for wider adoption. For example, the National Academy of Sciences conducted a report on the securitization of voting and concluded that science is not developed enough to support safe and credible internet elections and that blockchain is not sufficient to address security requirements attached to voting such as verifying identities of voters.[77]

Web3 is not without its critics, who can be dubious about its claims of decentralization or concerned that decentralization could magnify a host of societal ills. For example, a decentralized stock exchange would lack an emergency shutoff to prevent another Great Depression. Web3 is often described by skeptics as a solution seeking a problem, in particular due to its lack of clear use cases where decentralization would be superior to a centralized tool, yet billions of dollars in investment are pouring into Web3 startups seeking to use blockchain to solve modern problems. With millions of early adopters ranging from renowned

financial institutions to the government of El Salvador,[78] and interest from even the US government in establishing a central bank digital currency,[79] Web3 remains a critical emerging technology shaping the present and future.

BIODATA COLLECTION

Human biodata encompasses the vast amount of individual health and physiological data that internet companies now collect on their users. Traditional biometrics measure distinctive physiological or behavioral human characteristics. Some of the most notable include fingerprints; face recognition; iris or retina recognition; hand geometry; and behavioral identifiers like signatures and typing rhythm. Appropriate biometric measures must be universal across all ethnicities, distinguishable enough to be unique to each user, and permanent or constant enough that it can remain unique to the user.[80] The field requires the development of sophisticated algorithms to match characteristics accurately to different users, based on normalizing results against a massive data set.[81] Currently, biometrics authenticate identity and access control. The US government uses biometrics in immigration enforcement, terrorist identification, and potentially in the intelligence community.[82] Experts believe these unique identifiers are more reliable than knowledge or token-based security applications like passwords or passports because they are entirely unique to an individual. A passport or password can be forgotten or compromised, whereas one's fingerprint or facial features are constant.[83]

Biometrics are also used in gaming and virtual reality, often through haptic technology. Haptic technology uses biometrics and biological responses to simulate the range of sensations experienced through regular human interaction with the physical world. It recreates two primary sensations: tactile and kinesthetic.[84] The former includes sensations gained through the nerve terminals on the skin's surface, such as texture, temperature, and pressure, while the latter focuses on the perception of movement, force, and positioning.[85] Haptic technology stimulates the senses by applying various forces, vibrations, electrotactile stimulation, ultrasound or thermal stimulants, and chemicals to an individual's skin or muscles. It can be incorporated into wearable suits, vests, or other attachments.[86]

The haptics industry is rapidly growing. Market analysts forecast it to be valued at $4.6 billion in 2026, up from $2.6 billion in 2021.[87] Currently, the commercially available deployments of haptic technologies are largely confined to gaming and mobile devices to provide tactile feedback to users. For example, when a player gets shot or hit with an arrow at a specific spot in the game, that will trigger a vibration at the appropriately placed point.[88] While these suits make games more immersive, their adoption is dwarfed by traditional haptic deployments such as vibrating console controllers.[89] Social media companies have used vibrotactile technology in smartphones to drive user engagement. The platforms provide haptic feedback when a user likes a post on Facebook, Twitter, or Instagram, which makes users more likely to engage with content.[90] While these applications in social media are limited, the move toward convergence in social media and gaming through the metaverse may provide an opportunity for greater integration of haptic technology.[91]

Biometrics raise some serious concerns. Singular identifiers such as a fingerprint or iris scan can become compromised over time,[92] so some systems use a multi-layered approach for recognition that also incorporates a password or non-biometric identifier. When biometric signatures are compromised, it can be hard to reissue new identifiers or security provisions, because the data is intentionally unchangeable. Current research focuses on adaptive biometric systems which can help a database continuously update to changing biometrics. However, there are still many unanswered issues with this technology.[93] Among other concerns, the collection of such data can reveal personal medical information or, given the fallibility of

algorithms classifying the data, cause discriminatory bias through improper recognition or an inability to recognize certain features.[94]

In addition, biometric haptic technology may provide new implications for social media user identification. Biometric haptics record behavioral and physiological data in order to identify individuals based on their unique characteristics.[95] That data is then fed to an AI algorithm which would be trained to extract personally identifying features from the pattern of an individual's movements.[96] This application would allow continuous ID verification as users engage in immersive experiences. These are only the beginnings for the use of such data, as advanced extended reality and artificial intelligence technologies heavily rely on biodata to gauge your interest and consumer profiles.

Other forms of biodata, beyond biometrics and haptics, also have significant national security applications in the social media and internet contexts. DNA and general health data, collected by companies like 23andMe and even online searches for diagnoses or symptoms, can reveal immensely private personal information that people don't always know they are giving away.[97] Menstruation tracking apps raise concerns about evidence gathering to prosecute abortions in the wake of the Supreme Court overturning Roe v. Wade.[98] As electronic health records are made increasingly available directly to patients and easily transferrable, the sale of that aggregated yet personalized and detailed data to new phone applications (or even insurance companies looking to profile potential clients) is ripe for abuse. From a number of angles then, the integration of biodata collection into social media and internet platforms raises numerous potential concerns for the future. Biodata is a technological dark horse that may well transform user surveillance and targeting at a scale not currently imaginable.

CYBER INFRASTRUCTURE

Cyber infrastructure constitutes the final category, not so much because it is "emerging" as because the fundamental limitations of our infrastructure have significant implications for the future of social media and its attendant emerging technologies. In particular, issues of cybersecurity, connection speed, and general access proved salient.

Cybersecurity constitutes a relevant issue ironically for its *lack* of relevant technologies. Most small and medium-sized businesses lack strong cybersecurity protections — even those holding sensitive data, like dating app conversations or credit card information. There are few incentives for them to invest in security, either through liability or subsidies to help them pay the considerable costs for quality cybersecurity protections. This means that ransomware, theft, and other types of computer crime will remain rampant even as the available technology improves, until cybersecurity concerns are met. Hardware attacks and espionage also pose concerns.[99] Cyber attacks on critical infrastructure are already a critical national security concern, and as our national infrastructure becomes more digital, those concerns will only increase making the United States vulnerable to attacks from nation-states as well as criminal enterprises.

Complicating cybersecurity are structural complications. Cyberattacks involve multiple jurisdictions, and often cross state lines to fall under the jurisdiction of the Federal Bureau of Investigation (FBI).[100] Because local law enforcement does not have immediate contact with cybersecurity threats, they are not appropriately trained to deal with them. This leaves individuals and businesses often feeling powerless in the face of cyberattacks, as they approach local law enforcement for assistance. On a micro-scale this does not raise national security concerns. As cybercrime becomes more prevalent, though, and the US increasingly digitally-dependent, the risk increases. In fact, there are documented cases of (likely) nation state perpetrated cyberattacks that come to the attention of major private sector cybersecurity players, who then lack the effective convening powers to raise the alarms widely enough and to build consensus for ultimate attack

attributions to those nation states.[101] Although companies may have more freedom than the U.S. government to attribute attacks to particular actors, there is still a desperate need for more coordination between the government and threat analytics firms, particularly to amplify concerns when new attack vectors are discovered.

Beyond cybersecurity, technologies to increase mobile internet speeds will have significant implications for other emerging technologies. Mobile internet speeds are likely to skyrocket as 6G (sixth generation) mobile internet is introduced, and significant changes in adoption are already apparent from 5G (fifth generation) adoption. 5G mobile technologies both increase the speed of data transfer and improve the bandwidth between 4G technologies.[102] 5G is currently most prominent in discussions of autonomous vehicles, industrial machinery, and advanced robotics, while also having a significant impact on both military and commercial operations.[103] While 5G brings benefits, it also requires a focus on mobile security because there are more attack surfaces (more devices) and more traffic.[104] A study by Juniper Research found that in 2023, over 33 billion records were predicted to be stolen by cybercriminals from the US,[105] highlighting the importance of US emphasis on its own information defenses. Some experts believe that the US will set a global example of 5G network security not just through technology but also through policy and ethics,[106] although some are concerned that standard-setting bodies are vulnerable to undue influence from parties hostile to the US.[107]

On the home network side, the United States hosts a massive disparity in internet access that will severely limit the potential impact of 5G and eventually 6G, as well as any new internet technologies. Large swaths of the country do not have wired connections that can meet the Federal Communications Commission's 25 Mbps minimum speed.[108] Rural communities are often seen as the most afflicted by this problem and over the years the communities themselves either on their own through co-ops[109] or with help from government subsidies, have attempted to extend broadband services in rural communities. Recently, the Federal Communications Commission announced a $1 billion fund to support rural broadband in 32 states[110] and the Biden Administration added $10 million to be used to expand access to affordable, reliable, and high-speed internet services to Tribal Nations.[111] However, it is not just rural communities that don't have access to adequate broadband. Millions of urban families are entirely priced out of high-speed service.[112] As of June 2021, urban households without a broadband connection totaled 13.6 million while rural households totaled 4.6 million.[113] Lack of broadband is a serious concern when considering who will be able to reap the benefits of an increasingly digital future, from remote work to telehealth to recreation.

TECHNOLOGIES TO WATCH

While the five technologies thus far highlighted will play a key role in the evolution of the internet, there are numerous additional technologies to watch. In the future, for instance, satellites may play an important role enabling internet access and disaster response.[114] In fact, they already are in Ukraine, as they repel the Russian invasion.[115] While NASA and SpaceX are the most obvious candidates to launch satellites into orbit, several social media companies like Meta and Amazon have entered the space in an attempt to expand internet access to remote areas.[116] Amazon alone has committed $10 billion in order to launch over 3,000 satellites into low-Earth orbit by 2029.[117] These efforts are not without risks. Low cost commercial satellites may be launched without adequate cybersecurity protections or provisions for satellite maintenance, and foreign adversary suppliers can potentially compromise commercial satellites that gather sensitive information.[118] Space debris is another security concern — there are millions of pieces of junk flying in the zone of the Lower Earth Orbit (LEO) that range from flecks of space craft paint to parts of dead satellites, all traveling at incredibly high speeds.[119] Any contact with other space assets could lead to significant accidents, a problem only likely to worsen as more companies and governments launch objects into space.

Quantum computing similarly is worth mentioning because of the significant interest in the technology across both the public and private sectors worldwide. Quantum computing is a rapidly emerging technology, only a few decades old, that uses the laws of quantum mechanics to solve complex mathematical equations with superconductor quantum processors which are impossible for classic computers.[120] Current quantum problems include modeling the behavior of individual atoms in a molecule with different electrons interacting with one another.[121] If successfully developed, the quantum market could be worth billions of dollars, render all encryption useless, and cut through all resource constraints in artificial intelligence. It is highly speculative, however, and while it could revolutionize the internet and human computing power, it could also result in none of these things. Due to its unclear path to near-term adoption, we declined to include quantum computing in our assessments of the future of social media, though future similar endeavors may well take quantum into account.

Alternative energy and power grid technologies also have significant implications for the future of social media and the internet. As discussed in the previous discussion of cyber infrastructure, high speed internet access is a critical limiting factor in the growth of internet technologies. New forms of energy can offer easier, more stable access to all Americans, and can ensure that as internet energy usage spikes with more intensive technologies like virtual reality, power grids remain stable and energy production can match demand.[122] Power concerns, in terms of how that power is generated and how much is used or saved due to heavier internet usage, are also inextricably intertwined with climate change, a broader national security concern.

Semiconductors present hardware considerations to the debates around evolving internet and social media technologies. They are critical to electronic devices, and advanced semiconductors can be manufactured by only a handful of companies from an even smaller handful of countries. Recognizing the massive technological advantage they offer, the Biden Administration has restricted Chinese access to advanced American and other semiconductors, tightening the innovation supply chain.[123] The Chinese government reacted angrily and released plans to establish self-sufficiency in advanced semiconductor manufacturing,[124] but these interactions underscore the key role that semiconductors are likely to play in building the internet of the future. Semiconductors are widely regarded as a necessary precursor to innovation, so which countries and companies have them, in their most advanced iterations, will play a decisive role in which electronic devices proliferate in military applications and ultimately trickle down to consumers (or support innovations in other technological domains that trickle down).

While the Report previously discussed biodata collection, biotechnology as an entire field raises significant national security and societal concerns that can dovetail with advances in the internet. Crispr, mRNA advances, and other biotechnologies can contribute to personalization of the internet experience, including personalized drugs trumpeted by social networks. The same algorithms vacuuming up biodata from the internet or from home DNA kits are seen as one of the most promising new frontiers in drug discovery. As biotechnology introduces new and unproven medical treatments, patient communities on social media swap tips and advocate for their inclusion in new clinical trials, expanding the reach of biotechnology far beyond its current limits.[125] Entire medical research studies on rare diseases are conducted using patients sourced on social media.[126] New applications for the internet will crop up in biotechnology, just as biotechnology will symbiotically enable advances in internet targeting and extended reality technologies. The potential of this back-and-forth is both exciting, and in the wrong hands, potentially quite dangerous, offering yet another magnifying lens to the benefits and threats of the future internet age.

C. Major Threats

The Task Force identified six major threats in our current social media landscape likely to grow in the near future: information chaos; psychosocial and physical harm; lowered barriers for bad actors; loss of inno-vation; exploitation of power; and negative externalities. In some cases these threats magnify each other or come into tension. For example, while slowing the deployment of a technology in favor of added cyber-security measures could prevent physical or psychosocial harms, it also can critically slow innovation to a degree that risks both the development of the tech industry and the national economy. We note these harms extend across our online and offline lives, with different repercussions in each realm. Although our law enforcement and other systems focus on offline harms, as online life expands to encompass more human activity, distinctions will blur, and online threats may become equally important to counteract.

INFORMATION CHAOS

Modern digital tools allow everyone to be a content creator and publisher, with minimal barriers to entry and no verification filters. As a result, misinformation permeates the internet, generating information disorder and pollution. Our current system lacks accountability for malicious actors, be they authoritarian regimes, opportunists peddling lies, or angry mobs threatening or harassing an individual sharing a controversial opinion.

Part of this problem derives from lack of clarity in regard to rules for (1) what speech should be protected, given the global reach of platforms with conflicting speech jurisprudence; (2) who should decide; (3) who is liable for harmful content; and (4) how to review problematic content. The lack of clarity can corrupt the very concept of truth, as platforms struggle to make decisions with profound national security and public interest implications, particularly for vulnerable communities. More broadly, channels for accessing information are obscured by companies that maintain them, often without the full knowledge or understanding of the user. Tailored information feeds increase user engagement but also silos users into individually targeted echo chambers, which can promote false information and funnel users to more extremist positions without their knowledge or conscious acceptance.

One facet of this problem is the lack of ways to audit how large technology companies decide what content is banned versus not, as well as how they follow up when they get these decisions wrong. The public doesn't know how often unjust discrimination against the content of certain groups is detected, or how often a platform does detect misinformation and declines to act. The public gets no direct voice in what "unjust" banning means, which can hurt those with limited or different digital skills and funnel them to more extremist, misinformation-fueled sites. The public also can't quantify the harms that emerge from allow-ing misinformation to proliferate (measured e.g., in terms of money lost or even deaths). Without reliable, objective systems to understand the current environment, information chaos is exacerbated.

The harms play out in myriad ways. For example, individuals can be defined by past content that they created but which no longer defines them. Certain cultures have data voids in the knowledge they generate, which can be weaponized by political trolls or bad actors to promote disinformation. Reports of far-right

Chinese and Russian propaganda proliferating on Chinese-language WeChat threads and in Spanish-language news spread through WhatsApp demonstrate the pressing and insidious nature of this concern.[128]

In addition, while everyone can become content creators, companies limit the types of content, and the types of media that certain countries and certain groups can access, effectively restricting their information ecosystems. A troubling instance of this comes from China's new proposed social media law, that would effectively require vetting of all user-created content for conformity with Chinese Communist Party principles before it can post, which is likely to squelch unflattering viral news stories and many other forms of dissent.[129] Even without that law, we have already received reports of such censorship from dissidents, who complain that Chinese censors flag any form of Communist Party criticism as anti-Han Chinese racism. Much has been made in recent literature of the threats of information chaos, and new technology will magnify and transform these concerns.

PSYCHOSOCIAL AND PHYSICAL HARM

Social media usage, according to some research, can exponentially increase addiction and mental health issues like depression, stress, anxiety, and isolation. Reports of video game addiction and elective plastic surgeries skyrocketing in response to social media beauty trends highlight the significant health and economic impacts of such technology.[130] Cyberbullying, including death threats and stalking, is rampant online. As advanced AI targeting, virtual reality, and haptic suits enter the mainstream, they bring potentially more extreme addiction, physical, and psychological assault patterns, on and offline. For example, haptic suits enable wearers to "feel" stabbings or physical assaults. New forms of sexual harassment, including groping and "virtual rape," have already been reported in metaverse spaces. Psychosocial and physical harms from virtual experiences are here, with limited legal or other recourse for victims.

LOWERED BARRIERS FOR BAD ACTORS

The decentralization of technology, through its affordability and easy availability, brings the widespread ability to cause significant and large-scale physical, financial, and other damage. Already, small groups can inexpensively inflict great harm, through data theft, leaks of sensitive information, hacking, coordinated harassment or threats against an individual, real-world attacks or violent mobs organized online, and other means. New technologies will amplify these capabilities, as powerful algorithmic, blockchain, and other tools collide to offer criminals new attack vectors. Unfortunately, we lack systematic ways to identify, prevent, and counter such weaponization by criminals, which must marry an understanding of the criminal mind with an understanding of the technical nuances of these technologies.

Troubling examples of the ease with which the internet can facilitate crime abound. The previously mentioned weaknesses in cybersecurity and cyber infrastructure, including the lack of such measures for most companies and the lack of coordination to quickly communicate private sector-identified threats with the affected public, are just one source of weakness in our current leaky internet security protocols. Terrorist organizations use YouTube to recruit impressionable youths across the globe, encouraging them to travel to war zones or plan attacks in their home countries.[131] Scammers and harassers find ways to cajole or blackmail teens to send them naked pictures, using them as pornography and forcing the teens into sex trafficking.[132] Even rudimentary virtual reality games can train laypeople how to hijack airplanes, as one airport worker in Seattle demonstrated when, based entirely on knowledge built through a video game, he stole a plane and flew it into the ground as part of a suicide plan.[133] Gang leaders intimidate witnesses or the unaffiliated through social media postings.[134] While such actions can be undertaken even absent the internet, it introduces an unprecedented level of ease for those who engage in harmful activities. The tools themselves may be neutral, but as available online tools increase, so too will their abuse in new contexts.

LOSS OF INNOVATION

American military and economic strength depend on our cultivation of the leading edge of technological developments.[135] Especially as the private sector overtakes the public sector in critical technology investments that have direct national security implications, fostering the private innovation ecosystem is more important than ever.

Overregulation of industry risks undermining our position globally, as it can disincentivize investors and slow entrepreneurial development in industries where time is crucial. Innovators complain of a "compliance industrial complex," where our regulation has not kept up with the innovation needs and, while well intentioned in many situations, is now limiting our ability (either for larger companies or small) to innovate with things such as AI where authoritarian regimes and bad actors have limited impediments.[136] Changing dynamics in different technical fields require constantly evolving methods for generating innovation, and regulators often can't keep up. Heavy regulation favors larger companies, who have the financial cushion and internal resources to meet onerous rules that can stymie startups. A vibrant startup ecosystem allows a greater diversity of ideas to thrive, and too many rules can restrict who how designers envision future technology and who feels comfortable venturing into cutting edge spaces. Whether through federal research clouds or otherwise, there is a need for public computational infrastructure and public technology-related legal advice to help startups and other small players innovate in a safe manner on an even playing field.[137]

As arguably seen with some unicorn industries like ride-sharing,[138] flouting local regulations can be core to a company's early business model. But a society that rewards breaking the law renders its own laws useless. It incentivizes bad behavior, and only certain actors will play the game. Instead, innovation itself must be promoted as a strong public good, infusing all regulatory processes with an appreciation that stifling innovation can be the greater threat to society than other immediate harms concerning a regulator in the moment.

Beyond regulation, without sufficient structural supports for domestic talent cultivation and smart immigration processes to integrate foreign talent, the country's diverse, leading workforce will wither, losing ground internationally. An additional threat to American innovation is the consolidation of data and computational infrastructure in a few large companies. For example, as large data collectors limit access to the massive data sets necessary for training algorithms, innovations in AI are limited. The largest technology companies become functional gatekeepers for the types of AI innovations that they have most interest in seeing pushed forward, whether they intend such a role or not.

EXPLOITATION OF POWER

The power imbalance that exists in the physical world between large companies and consumers is exacerbated in the digital world, where the entire user architecture is privately owned. Although many services are offered for free, some tech companies harvest user data to generate revenue, selling user surveillance or user attention as their primary product. As a result, consumers/users (1) are susceptible to microtargeting, exploitation, and social/ political manipulation; (2) have limited control over their privacy and data security (and not all tech platforms are incentivized to provide security); and (3) cannot transfer their data between and to other platforms. Companies profiting from this user data economy face a strong tension, because this business model generates the majority of their considerable wealth and power, in addition to their value proposition for other stakeholders like small businesses looking to connect with customers.

The threat arises from the privacy, security, and other concerns that burden users under the status quo, though these concerns are not yet as pressing for many stakeholders. Debates around antitrust law touch on these issues, but skepticism abounds.[139] Some individuals appreciate that ads are tailored to their individual interests. Others suggest that privacy is no longer tenable, regardless of company activities. Instead, we should all learn to live in a more transparent world and better manage our individual data flows. At the same time, we are at the beginning of the power imbalance — as the internet takes over more of our lives, it is likely to grow.

The potential for manipulation via internet content is vast and growing at an extraordinary rate, with no transparency into the data needed to ascertain how effective it is likely to be in the future. Individuals have limited insight, at best, into how companies use their data and target them, cannot opt out of targeting, and face enormous hurdles to removing their data (even posted non-consensually) from these data sets or from online platforms, often entirely at the discretion of the platform.[140] In addition, large, aggregated data sets are surprisingly easy to deanonymize.[141]

As discussed earlier in this Report, we are not far from a time when companies can use an individual's biometric data to track their neural responses and target them based on biometric feedback about which they are not themselves aware. These companies already exert significant influence over user behavior, often impacting the most vulnerable in society. We see, for instance, young children dying due to dangerous online trends, trends their parents had no idea they were following.[142] Whether due to lapses in content moderation or intentional individual targeting for profit, the security implications of these tools as they improve are frightening. Scarier still, our current legal frameworks leave these powers unchecked.

NEGATIVE EXTERNALITIES

New technologies have resulted in new, unintended consequences for society. These impacts can be felt across diverse areas, and three that were consistently raised around social media and the internet were the erosion of journalism, climate change, and tax avoidance.

Shifting power dynamics in content creation, plus a 24-hour news cycle and internet publishing, have cratered the old business model of journalism. Quality journalism provides tremendous societal benefits that are not traditionally priced into news models — everything from an informed voting public to communal trust and accountability for politicians at all levels. This old model was supported by classified ads, which did not directly impact journalistic content. Many journalism experts cite the advent of Craigslist, and its gutting of classified ad revenue, as the first step in the industry's decline.[143] News aggregators and other automated news programs also detract from original content revenue streams, decreasing newsroom emphasis on costly investigative journalism and in-depth sourcing in favor of speed articles designed only for maximum exposure. Journalists in underserved parts of the world lack access to educational material that can help them to develop the needed digital skills to combat the new types of disinformation in their field. Struggle can breed innovation, and new forms of journalism like rural text message networks have the potential to improve access.[144] However, we encountered agreement across the spectrum: the current state of the industry is not sustainable, and social media and the evolving internet arguably catalyzed this latest round of challenges.

Big data and costly computational technologies, as well as utilization of existing technologies by an increasing share of the public, takes energy. Despite some material science research to alleviate those stressors,[145] current activities can contribute significantly to climate change and pollution, with the health and security concerns those entail. As seen with struggles around Russian sanction efforts over the Ukraine invasion, global dependence on fossil fuels already creates geopolitical challenges. Increased dependence brought

on by emerging technologies is a negative externality that must be dealt with before the next round of sanctions is rendered less effective by critical energy needs. If we want technological advancement to keep the same rapid development pace, energy efficiency is paramount.

As another example, multibillion dollar technology companies who grew through deficit financing and who creatively limit brick-and-mortar infrastructure can avoid paying taxes altogether.[146] Those taxes that are needed to fund both the functioning of American society which undergirds their businesses and solutions to the societal harms they inflict, intentionally or otherwise. Ultimately, our current society's structure does not consistently incentivize companies to act responsibly, with emerging unintended consequences to consider.

While the foregoing represent some of the most pressing concerns, potential harms will continue to present. The conversation cannot end here. Accordingly, the Task Force recognized the need to create frameworks that could support future efforts.

IV. Roadmap for a Healthy Digital World

VISION: A HEALTHY DIGITAL WORLD			
Foundation for Future Actions: Democratic Principles, Stakeholders, & Criteria to Evaluate Novel Solutions			
Pillars >	Effective Governance	Responsible Platforms	Empowered Public
Goals >	Research; Innovation; Accountability	Trustworthiness; Diversity; Respect for Rights	Education; Mobilization; Agency
Task Force Recommendations* >	**Fund Research and Grants to Address New Harms**	**Codify a Digital Bill of Rights and Developers' Code of Conduct**	**Foster Civic Education and Engagement**

Tools for Enactment:

1. Sample Digital Bill of Rights
2. Sample Developers' Code of Conduct,
3. Sample Information Governance Priniples

**All members of the Task Force have participated in their personal capacities and not on behalf of any other organization or entity. The recommendations in this section reflect the sense of the Task Force as a whole and are not attributable to individual members. They further reflect the diverse expertise of the members, who work on different aspects of the final recommendations.*

A healthy digital world is possible. With good leadership, the rapid evolution of technology brings immense promise to improve all our lives. The Task Force, accordingly, developed the following roadmap to help to provide the frameworks, action items, and tools necessary to address the national security and broader societal concerns raised by the rapid evolution of social media and the internet.

A. Foundation For Future Actions

In considering some of the most pressing concerns, the Task Force concluded that whatever solutions would be constructed, they would have to support the democratic principles at the heart of US governance. It would also be necessary to identify which actors have the capacity to influence change, and what criteria should be used to evaluate the most promising new solutions. This section explains the Task Force's approach and lays out its conclusions in each area.

DEMOCRATIC PRINCIPLES

The Task Force began step two of the deliberative process by asking what principles would be needed to protect a healthy digital ecosystem. The discussion, however, quickly shifted to the need to think more broadly than online communications. Task Force members of all political persuasions and areas of expertise raised concerns about the survival of American democracy itself. Fundamentally then, the Democratic Principles outlined by the Task Force answer the question, **"What principles are needed to maintain and foster a healthy democracy?"** Framed around online participation, the principles, below, infuse the Task Force recommendations and express the core values of this Report.

DEMOCRATIC PRINCIPLES TO PRESERVE

1. FREE EXPRESSION: The ability to express oneself without interference by a public authority is a treasured American freedom and a critical protection against authoritarianism. What today are considered bad ideas may be just that, but in both physical and virtual public squares, some of those unpopular ideas of today may become the cornerstones of public values tomorrow.

When internet platforms adopt the role of public fora, safeguarding free expression becomes more complex. Social media companies do not have the same constitutional obligations as the government and so have the ability to limit expression on their platforms as they see fit without violating the First Amendment. This can be a good thing, as content moderation reduces hate speech and weeds out mis/disinformation, a concept enshrined in 47 US Code Section 230, shielding internet platforms from civil liability over their hosted content. However, as individual platforms grow to encompass massive swaths of the virtual public square, their sheer size and opaque control of algorithms, removal of content, and increasing practice of deplatforming individuals and organizations–both alone and in conjunction with other online platforms–can have a profound impact on public debate. Free expression is a thorny concept, with its own internal inconsistencies, with which all potential solutions must grapple.

2. INFORMATION ACCESS: The ability to access information, including the information of one's choice, is an important facet of free expression that takes on added significance in the digital world. The most basic iteration of access is literal access to digital public spaces in the first place via an internet connection, and as internet applications become more resource intensive, a fast internet connection is also quickly becoming a necessity. In the modern age, internet access is necessary to provide true economic, social, and political participation, whether used for researching political issues or communicating with politicians. Unfortunately, equitable and affordable internet service for rural, socioeconomically disadvantaged, and marginalized populations remains elusive as commercial considerations drive how internet access is made across communities nationwide.

Information access is also a question of free expression and information integrity, as individuals need to be able to reach quality information to inform their opinions unencumbered by the filters of an algorithm's value judgements on what to show them. Companies, bad actors, nation states, and others with the economic means and abilities can increasingly dictate the information ecosystem of an individual without their conscious consent. As such, democratic independence and truly free choice in public decision making are threatened. A corollary to this access concern is access of input. When significant portions of the population lack access, they also lack the ability to create content from their perspectives, which limits the diversity of the internet and can skew interactions. For example, disproportionately large percentages of internet commentary are written by men, including movie reviews. The gender bias in reviews skews movie sites against those that target female audiences. Algorithms trained on internet-based language data sets are then overwhelmingly keyed towards male voices and concerns.[147]

3. INFORMATION INTEGRITY: The ability for citizens to rely on news, academic, and other sources of their choice for credible, trustworthy information is foundational to democratic decision-making. Democratic engagement requires citizens to be able to make decisions based on available information. Regardless of whether it relates to societal, political, economic, scientific, or other matters, that information must be reliable, accurate, and complete, and citizens must be confident that it is so.

That reliance can become problematic when a citizen's informational bubble is shaped by algorithms over which they have limited control or platforms which deliberately remove access to information and speakers outside of users' knowledge. Silicon Valley's own gurus have looked to "hook" users, adapting behavioral economics to form habits and subconscious cues that can direct individual behavior as a social media company wants.[148] Social media algorithms are essentially funnels to particular information. But, the funnels are dictated by the company's (or, if targeted, the bad actor's) goals, not by the individual citizen's goals. As a result, the information they provide may be more aligned with their advertisers' interests than their users' interests. As many critics point out, with many data and digital media companies, user behavior is the product. Platforms sell the ability to hook or alter that behavior.[149] If citizens are relying on social media for news and information, the integrity of what is presented to them is potentially compromised by the goals of the companies doing the presenting.

Even where a platform's intentions are entirely aligned with user goals, algorithms are susceptible to unconscious biases and human error. If the developer team harbors preconceived notions or lacks diversity, the problem magnifies. Under current models, an individual's confirmation bias will further magnify errors in their personal algorithm, as the more they "click" on news from a particular perspective, the more news they are shown that affirms that perspective. Such active bolstering of confirmation bias further lays the groundwork for authoritarian tendencies. Interestingly, this can only be demonstrated anecdotally — we can't see into the social media companies' algorithms that decide what content will be included in an individual's personal information bubble.[150] Citizens may benefit from understanding what is shown to them,

why, the dangers of confirmation bias, and how they can change their individual information bubbles to fit their own goals, rather than those of the companies selling their behavior.

4. COMMUNAL TRUST: Central to faith in democracy and its attendant political horse-trading is the idea that, at the end of the day, we are all on "Team USA," meaning we share a common set of values and beliefs that together form a national identity. Without these common norms, everything else falls apart. The societal cohesion that develops from community formation is critical to maintaining public trust in the wisdom of the crowd, as well as, preventing slides into chaos, on the one hand, and authoritarianism on the other. From this broad perspective, developing new relationships, sharing interests and values, exploring new possibilities, and enjoying leisure time, are all positive ways of finding and reinforcing commonalities and communion that further democracy through connection.

5. INCLUSION: Every vote matters, regardless of race, religion, gender, political views, sexual orientation, or ability. American democracy relies on collective action, and all are invited to participate. In the online context, inclusion can look different than in the physical world. Online threats and harassment, as well as the refusal to allow individuals to access online platforms or systemic economic forces that place such access out of reach, can stymie participation by marginalized populations, as can a lack of accessibility accommodations like screen-reader compatibility on webpages. As the digital world takes over more of our political, social, and economic lives, all people must be able to take part.

6. INSTITUTIONAL TRUST: Protecting democratic institutions and processes must be a key goal for all democratic governments. As many have noted, institutions are the foundation of progress, the base from which science and commerce can launch their creativity.[151] The loss of public faith in those institutions and processes can have violent consequences, as illustrated by the January 6, 2021 U.S. Capitol attack. The internet has played a significant role in eroding American institutional trust, through the amplification of conspiracy theories, the strengthening of extremist recruitment, and the destruction of respected information sources. Institutional trust must be earned, and where broken, rebuilt, but it should not intentionally be undermined. Allowing for questioning and scrutiny while countering mis or dis-information and thwarting malicious actors is a difficult but vital task.

7. SECURITY: Citizens need to feel safe in order to participate in voting processes, reflect on issues of import, and otherwise contribute to a democratic society. More than a democratic principle, the safeguarding of citizen health, be it physical, mental, or otherwise, is a critical component of any social contract between citizens and government. The enactment of legal protections tends to be reactive, not proactive. This is particularly true of digital users who increasingly need protection from both virtual and physical harm. Legal protections are not comprehensive. The laws and law enforcement coordination around cyberstalking, revenge porn, cyberflashing, doxxing, phishing, hacking, and other internet threats, are a patchwork. As these threats evolve and disproportionately thwart internet participation by certain populations, providing new forms of security to all becomes a critical democratic issue.

8. PRIVACY: Privacy in one's beliefs, thoughts, emotions, and sensations fosters personal development, self-reflection, and intellectual inquiry. It protects a sphere of intimate relationships and allows users to express themselves outside of the public eye. It also provides users with the space to learn about, debate, and decide how to approach matters that democracy requires its populace to address. Some users may be willing to divest themselves of certain matters related to privacy insofar as convenience and services can be better delivered when data is shared. And some invasions of privacy are sanctioned in the interest of security. But not all individuals are comfortable with these approaches. Just as privacy and other rights are constitutionally established to protect minorities, so too does the ability of users to engage online while still being able to mediate their bounds of intimacy and knowledge about their own behavior matter.

The stakes are high. Democracy cannot exist without dissent, and privacy creates the conditions for dissent to arise and thrive, within and among individuals as well as when people inject controversial ideas into the discourse. Dissidents of authoritarian regimes demonstrate this privacy imperative. Our discussions with international activists underscored how the ability to mask physical identity enables them to develop and spread messages through social media and the internet. One activist, concerned about their own unmasking on certain platforms, recounted how the Chinese government pressured a social media platform to remove posts critical of the Communist Party over complaints of anti-Han Chinese racism.

In the privacy sphere, social media platforms are faced with difficult choices around squashing fake accounts, sharing user data with advertisers, responding to government inquiries, integrating privacy into products without impacting user experience, and other concerns. Whether that status quo should continue is a matter of much debate.

9. TRANSPARENCY: Public decision-making by those acting on the government's behalf facilitates democracy. Voters' and citizens' decisions, in turn, require information — not simply data, but whole data sets within the appropriate context. Transparency is critical to good governance and avoiding corruption.

As internet platforms play increasingly large roles in our lives and create new societal problems with which the public must grapple, private sector transparency becomes important as well. Algorithmic transparency, for instance, frequently arises as a critical emerging concern. It incorporates insight into how data is collected and analyzed, the contours of data sets employed to train algorithms to their tasks, and how the algorithm undertakes decisions and makes value judgements (the most technically difficult to achieve). And competing concerns present: as discussed above, the privacy and safety of dissidents must be weighed as a danger of transparency misuse. The degree and extent of both the current and requisite future private sector transparency is debatable, but there is wide agreement that more transparency is needed to inform public decisions on emerging technology and our future.

10. ACCOUNTABILITY: The legal maxim that "rights warrant remedies" applies as a broad democratic principle. In a functioning democracy, bad actors and even well-meaning actors who cause bad consequences are held accountable for their impacts on society. As technology rapidly evolves, the law struggles to keep pace. That is no reason to sideline either the judicial concepts of fairness and equity, however, or the remedies that enforce those concepts. The question of who should enforce compliance, particularly in internet spaces untethered from the physical world, remains open.

ACTORS FOR CHANGE

To whom should we turn for help in shaping a more secure digital future? To answer this question, the Task Force considered the roles of over 80 different entities within the social media and internet ecosystems. Each offers different ways to guide the positive development of emerging technologies and the internet. We catalogue them here as a basis for determining the most effective avenues for enacting future needed changes, with brief explanations of government actors with whom the reader may be unfamiliar.

Collectively, we identified over 120 different types of actions these actors could take today, from realigning government procurement programs to locally sponsored hackathons, that might move the needle on the concerns raised in this Report. The specifics of that list are not as important, although we are happy to make it available upon request, because the available actions will change over time far more quickly than the actors with interests in the space. Rather, here is a "first stop" for answering future questions of what can be done. This section attempts to answer the more fundamental question of who might do something.

ACTORS FOR CHANGE IN SOCIAL MEDIA AND THE INTERNET			
GOVERNMENT		**PRIVATE SECTOR**	**CIVIL SOCIETY**
National Security-Focused Federal Agencies	Department of Homeland Security	Internet Platforms	Journalists and Media Organizations
	State Department	Telecommunications Companies	Nonprofits
	Department of Defense	Technology Startups	Consumers
	Intelligence Community	Financiers	Foundations
	Federal Communications Commission	Influencers	Universities
	DOJ/NSD	Coding Academies	Libraries, Museums, and Other Civic Education Groups
	FBI	Small and Medium Sized Businesses	Grassroots Organizers
Communications and Commerce-Focused Federal Agencies	Federal Trade Commission	Large Corporations	Professional Organizations
	Federal Communications Commission	CEOs and Other Leadership	Chambers of Commerce
	Securities and Exchange Commission	Employees and Employee Resource Groups	K–12 Schools
	Commodities and Futures Trading Commission		
	Consumer Financial Protection Bureau		
Other Relevant Federal Agencies	Federal Reserve		
	Department of Treasury		
	Department of Agriculture		
	Health and Human Services		
	Department of Education		
Other Government Entities	State and Local Law Enforcement		
	Federal Judiciary		
	State and Local Judiciaries		
	Congress		
	State and Local Representatives		
	White House Offices		

NATIONAL SECURITY FOCUSED FEDERAL AGENCIES

DEPARTMENT OF HOMELAND SECURITY (DHS): The DHS is home to many relevant agencies that monitor the cyber domain, key among them being the Cybersecurity and Infrastructure Security Agency (CISA). CISA focuses on managing risks to the U.S. cyber and physical infrastructure and coordinates the execution of our national cyber defense, including asset response for significant cyber incidents and sharing information across government and private sector partners.[152] For example, CISA's National Risk Management Center (NRMC) contains a "Mis-, Dis-, and Malinformation (MDM) team" which aims to build national resilience to MDM and foreign influence activities in close coordination with interagency and private sector partners, such as social media companies, academia, and international partners.[153] Within the government, MDM works in close collaboration with the FBI's Foreign Influence Task Force, the U.S. Department of State, the U.S. Department of Defense, among other agencies, to recognize, understand, and help manage the threat and dangers of MDM and foreign influence. The MDM team also works with the DHS Privacy Office and the DHS Office for Civil Rights and Civil Liberties to carry out its guiding principles of "protection of privacy, free speech, and civil liberties."[154]

While CISA itself can conduct investigative activities, the DHS has its own federal criminal investigative arm for law enforcement purposes known as Homeland Security Investigations (HSI) which can oversee cybercrime.[155] The DHS's U.S. Secret Service also has Secret Service agents in the Cyber Operations, Criminal Investigations and Investigative Support divisions which work to protect and prevent U.S. businesses from computer and cyber crimes.[156]

The DHS also includes the Cyber Safety Review Board, which was established pursuant to President Biden's Executive Order 14028 on "Improving the Nation's Cybersecurity."[157] The Board's role is to review major cyber events and make recommendations for improvements within the private and public sectors.

Other DHS entities of interest include the DHS' Science and Technology (S&T) Directorate. Within that directorate, there is funding for cyber security education in K-12 and higher education, collaboration with research development centers, industry, other agencies, international partnerships, national laboratories, and higher education, and independent and collaborative research.

STATE DEPARTMENT: Though the State Department primarily focuses on U.S. relations with countries abroad, it plays a key role in the effort to set responsible online standards internationally. The State Department's Global Engagement Center's (GEC) mission is to direct and coordinate federal government efforts to recognize and counter foreign state and non-state propaganda and disinformation efforts aimed against the United States and its partners.[158] GEC also contains the Technology Engagement Team which convenes technology experts and programs from private and public sectors to drive innovation against foreign disinformation.[159]

The State Department also has a cyber bureau which has gone through various iterations over the past several administrations.[160] In the 117th Congress, Congress passed the Cyber Diplomacy Act of 2021 to direct the State Department to create a Bureau of International Cyberspace Policy to lead the Department's diplomatic cyberspace efforts, including efforts on cybersecurity, internet access and freedom, the digital economy, among other specified duties and responsibilities. The President is also directed to create a strategy to engage internationally to promote norms to establish responsible state behavior in cyberspace.[161] The Bureau of Cyberspace and Digital Policy (CDP) was established on April 4, 2022, with the stated mission of addressing the "national security challenges, economic opportunities, and implications for U.S. values associated with cyberspace, digital technologies, and digital policy."[162] The bureau's three

policy units include the International Cyberspace Security, International Information and Communications Policy, and Digital Freedom.

DEPARTMENT OF DEFENSE: Inclusive of the nation's military and intelligence agencies,[163] the largest executive branch agency contains a multitude of offices and branches which work on cybersecurity. Militarily, the Defense Department contains the Cyber Command (CYBERCOM) combatant command with the mission to "direct, synchronize, and coordinate cyberspace planning and operations, to defend and advance national interests in collaboration with domestic and international partners."[164] Of the intelligence agencies, the most cyber-focused is the National Security Agency (NSA) to strengthen national defense and secure national security systems.[165]

INTELLIGENCE COMMUNITY: The Office of the Director of National Intelligence (ODNI) is heavily involved in emerging technologies and the internet, and in 2022 released the FY2022-2026 ODNI S&T Investment Landscape, a document mapping out investment plans for key areas of focus for the intelligence community between 2022 to 2026.[166] Key areas include artificial intelligence, data, cyber, computing, and sensor capabilities, and their applications span from basic tools to complex technologies for national security/military use that require government participation.[167] On social media specifically, the ODNI noted tools to "rapidly discover and analyze highly diluted information on social media."[168]

In-Q-Tel (IQT) is a CIA-backed venture fund investing in technology startups for the purpose of delivering emerging technology to the U.S. government.[169] Focusing on dual-use technologies (commercial and national security) in its evaluation of more than 2,000 startup companies annually,[170] IQT's investments bring together government partners to maximize cross-collaboration in research.[171] IQT Emerge, a new effort, now seeks to commercialize technology by government funded initiatives to address national security needs.[172]

DEPARTMENT OF JUSTICE: The Department of Justice, including its Federal Bureau of Investigation (FBI), can work in coordination with other agencies to carry out its law enforcement functions in criminal investigative matters.[173] Within the agency, divisions monitoring cyber crime include the National Security Division (NSD) and the Criminal Division's Computer Crime and Intellectual Property Section (CCIPS).

COMMUNICATIONS- AND COMMERCE-FOCUSED FEDERAL AGENCIES

FEDERAL TRADE COMMISSION (FTC): The FTC's mandate is primarily to investigate and prevent unfair methods of competition or deceptive practices affecting commerce.[174] The FTC executes its mandate through investigation, enforcement (alongside the Department of Justice), and rulemaking to protect con-sumers and competition. The FTC's mandate and authority extends to key emerging technology issues including data privacy, cybersecurity, and antitrust practices by big tech companies.[175] The current FTC Chair, Lina Khan, has outlined that the FTC's strategic approach will include "being attentive to next-gen-erational technologies."[176]

THE FEDERAL COMMUNICATIONS COMMISSION (FCC): The Federal Communications Commission regulates interstate and international communications by radio, television, wire, satellite and cable in all 50 states, the District of Columbia and U.S. territories. An independent U.S. government agency overseen by Congress, the commission is the United States' primary authority for communications law, regulation and technological innovation. In its work facing economic opportunities and challenges associated with rapidly evolving advances in global communications, the agency capitalizes on its competencies in: (1) Promoting competition, innovation and investment in broadband services and facilities, (2) Supporting the nation's economy by ensuring an appropriate competitive framework for the unfolding of the communications

revolution, (3) Encouraging the highest and best use of spectrum domestically and internationally, (4) Revising media regulations so that new technologies flourish alongside diversity and localism, (5) Providing leadership in strengthening the defense of the nation's communications infrastructure.

Of note, the FCC's Working Group on Artificial Intelligence and Computing report emphasized the benefits of wide scale deployment and adoption of artificial intelligence (AI) and machine learning (ML) as an integral part of the nation's telecommunications systems.[177]

THE SECURITIES AND EXCHANGE COMMISSION (SEC): The SEC's tripartite mission is to (1) protect investors; (2) maintain fair, orderly, and efficient markets; and (3) facilitate capital formation.[178] The SEC Executes its mandate through investigations and enforcement and rulemaking. With respect to online social interactions, the SEC takes the lead on determining whether emerging technologies, such as cryptocurrencies, stablecoins, decentralized finance technologies, or Initial Coin Offerings (ICOs), are subject to securities law. In the last five years, the SEC has established several new offices to specifically address emerging technologies. The SEC has also pursued enforcement actions aimed at curbing the abuse of blockchain, a technology many argue enables criminals to more easily evade investigation and enforcement, and in providing guidance or fines for the use of social media interaction, such as for the sharing of misleading statements.

THE COMMODITY FUTURES TRADING COMMISSION (CFTC): The mission of the Commodity Futures Trading Commission (CFTC) is to promote the integrity, resilience, and vibrancy of the U.S. derivatives markets through sound regulation.[179] The CFTC set a 2020-2024 strategic plan committing itself to addressing both the risk and opportunities arising from "21st century commodities,"[180] and the Commission plans to develop a framework promoting responsible innovation in digital assets. While its regulatory oversight authority over commodity cash markets is limited, the CFTC maintains general anti-fraud and manipulation enforcement authority over virtual currency cash markets as a commodity in interstate commerce.[181] A recent "flurry" of activity charging entities for offering cryptocurrency derivatives and margin trading without registering as futures commission merchants (FCMs), appears to have market observers viewing the CFTC differently, reporting, "[w]hile the CFTC has issued regulatory guidance in the past and engaged in some regulatory enforcement activities, it has now established itself as a key regulator of the industry along with the US Securities and Exchange Commission (SEC), the US Department of Justice (DOJ) and the US Department of the Treasury (Treasury)."[182] In 2017, then CFTC Chair Mr. Giancarlo affirmed the agency's commitment to "facilitating market-enhancing innovation,"[183] and announced the launch of LabCFTC, an internal FinTech lab increasing CFTC accessibility to innovators, while enhancing the CFTC's understanding of new technologies for upcoming policy initiatives in the space, such as AI.

CONSUMER FINANCIAL PROTECTION BUREAU (CFPB): The Consumer Financial Protection Bureau (CFPB) is a relatively new agency created in 2010 to promote innovation, competition, and consumer access to financial services. The Bureau engages in investigations and requests information from covered persons, issues subpoenas or civil investigative demands, conducts hearings and adjudication proceedings, and commences civil actions in federal court seeking any appropriate or equitable relief against any person that violates a federal consumer financial law.[184] The CFPB has solicited public feedback on how Big Tech may leverage existing online dominance to rapidly scale the use of digital payment networks, including cryptocurrencies. This request for public input followed CFPB orders to Google, Apple, Facebook, Amazon, Square, and PayPal concerning their plans and practices regarding payments. The CFPB has also indicated it is monitoring and preparing for increased consumer adoption of cryptocurrencies to respond to cases triggering its obligations under federal consumer financial protection laws and will study

Chinese payment platforms, including Alipay and WeChat, to better understand system practices and inform the agency's work.[185]

OTHER KEY GOVERNMENT ACTORS

FEDERAL RESERVE: Initiatives include initiating discussion and soliciting public comment on central bank digital currencies and developing clear and consistent standards for assessing financial institutions' cyber security preparedness.

DEPARTMENT OF TREASURY: Initiatives include taking actions to disrupt criminal networks and virtual currency exchanges responsible for laundering ransoms, encouraging improved cyber security in the private sector, increasing incident and ransomware payment reporting to U.S. government agencies, and hosting financial innovation roundtable events.

US DEPARTMENT OF AGRICULTURE (RURAL BROADBAND): Initiatives include e-Connectivity for all rural Americans and the COALESCE program (a focus on operations of cyber-physical systems for farming, like sensing, modeling, and decision-making at the level of individual crops).

HEALTH & HUMAN SERVICES (HHS) (CENTERS FOR DISEASE CONTROL): Initiatives include strengthening the agency's core IT capabilities to promptly provide access to information to inform decisions when time is critical, modernizing its IT infrastructure, current systems, and tools, and developing advanced analytic capabilities; and ensuring more effective cybersecurity.

DEPARTMENT OF EDUCATION: Initiatives include adult digital literacy, strengthening cybersecurity education in high schools, and cyber security in professional and higher education (supported by federal and state departments of education and other federal agencies).

LOCAL LAW ENFORCEMENT: Local police generally play a limited role in social media and internet related crimes, because they are typically cross-border in nature. That said, local law enforcement officers typically use social media for three purposes: (1) communication, where law enforcement can publish bulletins and their contact with the public; (2) investigation, where agents use public social media to gather evidence of criminal activity; and (3) intelligence gathering, where law enforcement obtain information about user activity as a form of broad monitoring.[186]

CRITERIA TO EVALUATE PROPOSED SOLUTIONS

Recognizing the novelty of addressing national security concerns through broader societal contexts, the Task Force established the following criteria to guide strategic decision-making as part of step six of the deliberative process: evaluating proposed solutions. The primary criterion of the Task Force to guide the national security focus of the solutions was to support the previously discussed Democratic Principles. The other criteria offer a broader emphasis on policy efficacy important to balance across a variety of stakeholder interests.

1. **SUPPORT OF DEMOCRATIC PRINCIPLES:** The degree to which a solution bolsters the Democratic Principles outlined above. The Task Force considered this criteria of paramount importance.
2. **FEASIBILITY:** The degree to which a solution can be effectively implemented. This may depend on:
   - the number of actors and complexity of the processes involved in agreeing to and implementing the solution (recognizing that enacting laws or policies can quickly become mired in bureaucracy);
   - whether those actors have conflicting interests or the processes require expending significant political capital;
   - the cost of implementing the solution, including the extent to which a solution uses existing building blocks and resources (e.g., infrastructure, processes, frameworks, legal principles, and/or institutions);
   - the degree to which or likelihood end users will embrace the change (e.g., usability, user experience, convenience);
   - capacity of enforcement; and
   - how long it will take to actually implement the solution.
3. **OPPORTUNITY FOR IMPACT:** The degree to which a solution will meaningfully address the worst harms. In addition, the degree to which a solution accomplishes its intended purpose. We can't nibble around the edges.
4. **SPEED:** The degree to which a solution represents a quick win, including to help incentivize further governance actions. The general sentiment adopted was that we need to start somewhere: we can't dither while Rome burns.
5. **INNOVATIVENESS:** The degree to which a solution presents a new way of tackling a hard problem; on the other hand, innovative solutions are sometimes untested. We want to do more than reinvent the wheel.
6. **BENEFIT PRESERVATION:** The degree to which a solution supports, fosters, or otherwise leaves intact social media's benefits. In addition, the degree to which a solution might extend or enhance those benefits. Don't throw the baby out with the bathwater.
7. **EVERGREEN:** The degree to which a solution is flexible and/or sustainable enough to be relevant in governing future technologies and attendant risks. Tech changes every 2-3 years. The most effective solutions will last beyond the latest innovation.
8. **AVOIDANCE OF COLLATERAL DAMAGE:** The degree to which a solution minimizes unintended consequences, including bypassing or manipulation by bad actors. One way to measure the likelihood of collateral damage is to assess the degree to which a solution is informed by and involves a range of stakeholders.
9. **POLITICAL WILL:** The degree to which there is widespread consensus and agreement on the fundamental problem and the pressure on / willingness of key actors to address it. "We need enough, and the right, people at the table to make it happen."

B. Recommendations

TASK FORCE RECOMMENDATIONS* *Policymakers should identify and codify protections against harms that apply to the digital world, and provide funds for research and grant programs for investigating and responding to those challenges.*		
EFFECTIVE GOVERNANCE:	**RESPONSIBLE PLATFORMS:**	**EMPOWERED PUBLIC:**
Policymakers should identify and codify protections against harms that apply to the digital world, and provide funds for research and grant programs for investigating and responding to those challenges.	Industry, civil society, academia, and the public should develop a users' digital bill of rights and a developers' code of conduct, and promote their adoption and adherence.	All stakeholders, including government, platforms, community groups, academia, and civil society, have an obligation to educate and provide tools to online users so they are empowered to think critically, to advocate for their interests in the digital world, and to participate in democratic processes.

**All members of the Task Force have participated entirely in their personal capacities and not on behalf of any other organization or entity. The recommendations put forward are not attributable to any individual members. Not all members work directly on, or profess expertise in, all of the recommendations set forth below; nevertheless, this set of recommendations reflects the sense of the Task Force as a whole.*

Applying the aforementioned framework to potential solutions to our current problems, the Task Force whittled approximately 80 ideas down to the three current recommendations, organized by their promotion of effective governance, responsible platforms, or an empowered public. Each recommendation is keyed to one of the three pillars of the American digital ecosystem: (1) effective governance mechanisms, (2) responsible platforms, and (3) an empowered public.

Each pillar must possess three hallmark qualities to succeed in its digital world role, which are termed its goals. The Task Force-endorsed recommendations are intended to guide efforts within each pillar to meet its goals. The compendium of further concrete steps to reach those goals draws upon the Task Force's collective expertise. These recommendations cover myriad actors in society, reinforcing the need for creative collaborations, including many that exclude government altogether, in the name of national security and democracy.

EFFECTIVE GOVERNANCE

TASK FORCE RECOMMENDATION *Policymakers should identify and codify protections against harms that apply to the digital world, and provide funds for research and grant programs for investigating and responding to those challenges.*	
GOALS	**POSSIBLE STEPS TO ENACTMENT**
Research	Federal Research Consortium
Innovation	Early Stage Grants
Accountability	Disclosure and Reporting Requirements

The digital world fundamentally alters the relationship between government and society, rendering our current governance authorities inadequate. The internet creates new, loosely governed spaces and interactions that will create new security challenges that will only expand with the advent of new technologies. Policymakers and regulators currently lack the coordination, authorities, information, and resources to effectively safeguard a positive digital future. Although these recommendations focus on the federal government, the same is true of investors, funds, boards, entrepreneurs, and executives who are involved in effective governance on the private sector side. Digital Rights require protections our current structures do not fully offer. Ultimately, we need a broader governance framework to enhance our national security.

GOALS: We need governance that 1) fosters research, 2) encourages innovation, and 3) enhances accountability.

New technology exists at the cutting edge of knowledge. To properly understand how to best manage its consequences, government regulators need reliable research. Government must also adapt to this flexible environment, supporting private innovation and bringing some innovation in-house to bolster the public interest. Finally, good governance will bring accountability for the missteps and bad actors in the space, as good policy only succeeds where fairly and consistently enforced.

RECOMMENDATION: Policymakers should identify and codify protections against harms that apply to the digital world, and provide funds for research and grant programs for investigating and responding to those challenges.

As civil society works to prioritize and clarify the principles that are important to a healthy digital society, such as proposed in the Digital Bill of Rights, policymakers should watch and consider what policies, rules, and laws may be needed to realize the full public benefit of these principles. A bipartisan Congressional Commission, Federal Advisory Committee, or other executive branch body should be created and staffed by representatives from industry, government, academia, and civil society to conduct extensive research into emergent online harms and necessary regulatory protections. Its recommendations should cover issues including data transparency, information quality, security, data ownership, necessary platform disclosures, maintaining American competitiveness, accessibility and inclusion, and opportunities for public-private partnerships, with consideration of potential comprehensive legislation. In light of the rapid advancement of new and emerging virtual technologies blending the digital and physical worlds, the laws and policies proposed by the body must be technology neutral.

1) Establish Federal Research Colloquium

As part of their recommendations, the body should pay particular attention to identifying the most fruitful avenues for future research and grant programs, whether distributed through existing executive branch programs or through new organizations. A primary pathway to a coordinated funding program could be, via the NSF or NIH, a research consortium on digital harm. Alternatively, the Consortium could be housed within Federally Funded Research and Development Centers (FFRDCs) already serving the DOD.

Moreover, Congress should direct the FTC to clarify when and how platforms can share data with researchers from academia and civil service while protecting user privacy rights. Research should focus on establishing definitions and baselines for harms (including psychological harm); effective reporting mechanisms for user safety issues; developing an open research training data set for researchers at higher education institutions; convening discussions on standardizing data quality; understanding and publicly sharing the impact of automated decision-making; and experimenting with technology that supports democracy and transparency principles, rather than simply creating technology for government use; among other topics.

2) Distribute Early Stage Grants to Encourage Innovation

In addition, the body should specifically explore funding programs to incentivize companies or early stage investors to adopt practices that promote democratic and information governance principles (like those discussed in this Report) and Digital Rights (see discussion, infra, for potential rights to be taken on board). In those areas of science and technology where innovations are still unproven or may not be immediately profitable, the government could fund companies or emerging venture capital funds that seek to promote the aforementioned principles. Through such research and grant programs, the government can explore the most promising avenues for new regulation.

3) Undertake Study and Establish Disclosure and Reporting Requirements for Enhanced Accountability

The first step towards accountability is to understand the current social media landscape, the baseline of regulatory authorities, and the regulatory needs of relevant State and Federal agencies, which the previous emphases on research and innovation aim to do. Building on that work, government agencies will need to define and promulgate rules for mandatory platform disclosures and reporting, including based upon standardized information governance (as outlined earlier in this Report) principles, perhaps drawing structural inspiration from models in the investor realm that currently rely on environmental, social, and governance principles. To expedite implementation, relevant federal agencies like the SEC and FTC (in conjunction with private industry, research community, and national security leaders) could be asked to develop disclosure and reporting requirements under existing regulatory frameworks, public and non-public, for all digital media and platform companies. They should also explore whether new authorities requiring legislation are needed.

Topics that they should consider for disclosure and reporting requirements include standardized democratic social norms, transparency of algorithms and automated decision-making, data sharing with researchers, business practices monetizing user data, and evaluating current health and systemic risks, among other topics. For example, they should report on the incidence of foreign government-sponsored or -amplified postings on their platforms, and if they cannot provide such information, they should explain in detail why not and the steps that would need to be taken to glean that. Such efforts must take into account that all government reporting required by the United States will pressure social media companies to share that same data with authoritarian adversaries. Given the demonstrated ease of de-anonymizing aggregated data sets that could be used to target dissidents, government agencies must take great care in what information they ultimately request through reporting. Although there is much flexibility in how, the government must take a more active role in ensuring a healthy digital world.

RESPONSIBLE PLATFORMS

TASK FORCE RECOMMENDATION *Industry, civil society, academia, and the public should develop a users' Digital Bill of Rights and a Developers' Code of Conduct, and promote their adoption and adherence.*		
GOALS	**POSSIBLE STEPS TO ENACTMENT**	
Trustworthiness	Interagency Working Groups with Formal Channels for Public Input and Education	Self-Regulatory Industry Collaborations around Information Governance Principles or Other Ethical Standards
Embrace Diversity	Support for Diverse Employee Perspectives and Inclusion Work, Particularly to Support Content Moderation and Safety Efforts	
Respect for Digital Rights	Company Training	Formal Commitments to a Digital Bill of Rights and Developers' Code of Conduct

Emerging technology gives internet platforms an outsized role in societal interactions, for which they are not currently well-suited. The internet's role in our daily lives is growing faster than even some of its most sophisticated platforms can manage. The situation will become more pronounced as extended reality and decentralized technologies come of age and platforms that are already well-established will have advantages that may help them achieve market dominance. Society expects more from companies, as well as their investors, with their increasing acquisition of power. Simultaneously, history has shown the importance of ensuring a greater role for consumers and consumer protections. As significant portions of the public square move into private hands, platforms must adapt to new public responsibilities.

GOAL: We need platforms to exhibit 1) trustworthiness, 2) high ethical standards, and 3) respect for users' digital rights.

Platforms must gain the trust of consumers by judiciously and equitably enforcing their policies, aligning their incentives with user interests, and presenting trustworthy information. This does not mean that platforms must be the ultimate arbiters of truth; instead, transparency and empowering users to decipher credibility are two key factors in gaining the public's trust. Responsible platforms will also set high ethical standards internally, both for their employees and for their broader business decisions. As platforms receive tremendous societal power and space to innovate without onerous government regulation, they must also commit to ethical standards to curb abuse of that power and discretion. Part of this commitment encompasses the need for platforms to educate the public about how their algorithms work so the public can truly oversee their interests in the digital world. Finally, platforms must honor the digital rights of all their users — a critical component to continue their positive relationship with American society.

RECOMMENDATION: Industry, civil society, academia, and the public should develop a users' Digital Bill of Rights and a Developers' Code of Conduct, and promote their adoption and adherence.

The Digital Bill of Rights and Developers' Code of Conduct provide model norms and standards that could be adopted by the producers of digital society and used to inform their policies. They are intended to focus the attention of industry, civil society, academia, the public, and the government at every level in order to produce a better coordinated all-society strategy for a healthy digital universe. For example, even regulators could use them in guiding enforcement actions. Critical topics to address include public reporting and data disclosures that could help facilitate transparency of algorithms and automated decision-making, algorithmic auditing, portability or interoperability standards, data sharing with researchers, ways

to measure the credibility/accuracy in original content, accessibility and inclusion, ethical safeguards for business practices monetizing user data, and evaluations of current health and systemic risks.

1) All-Society Digital Strategy Should Be Adopted to Bolster Platform Trustworthiness

In order to be credible and, therefore, effective, such an all-society strategy for a healthy digital society will need to be drafted using a process that avoids giving any company an economic advantage. It must create space for new entrants and avoid a monopoly of power for any single large platform. This all-society digital strategy for a healthy digital society could grow from interagency working groups at the federal, state, and/or local levels, with representatives from the major online platforms, as well as representatives from smaller startup companies, civil society, and academia. Developing these norms and standards will require opening formal channels for public input, engaging community and advocacy groups in dialogue, and ensuring the perspectives of minorities and vulnerable communities are heard. The seeds for leadership of such an effort already exist across a number of federal agencies, including the FCC and FTC, for example.

Additional efforts at norm or standard-setting could be based on successful efforts to develop the EU Code of Practice on Disinformation, which has brought together online platforms and the advertising industry to self-regulate. Industry undertook a similar effort in Australia, as this model seems to be gaining favor as an initial step. An all-society effort requires engagement in a multitude of ways at different levels of specificity to generate buy-in and operationalize the new norms and standards on the ground.

Building off current efforts in the finance industry that reward company adoption of responsible environmental, social, and governance (ESG) principles, a set of information governance principles could hold platforms to ethical account via private sector pressures. Combined, if so desired, stakeholders could develop a tech industry-focused set of ESIG standards (with the "I" standing in for "Information Governance"). ESIG criteria could become part of defined guidance for companies, help individuals evaluate which technologies to use, help government assess procurement partners as part of competitive grant and contracting processes, and help investors evaluate companies for investment.[187] *The Task Force developed an illustrative set of Information Governance Principles, included later in this Report.*

Much like the SEC enabled the private sector in the 1940s to develop its own practices that were eventually codified into law, the tech industry should be encouraged to set its own standards that promote the essence of ethical information governance principles.[188] In fact, robust self-regulation is in the industry's best interest. As pointed out to us by the CEO of a major advertising enterprise, self-regulation can even persuade Congress against regulating an industry altogether, as in certain corners of direct selling and direct marketing.[189] Information governance principles, or ESIG more broadly, would better equip investors to gauge risks posed by internet platforms and provide a common basis for the industry to codify appropriate behavior.

2) Embrace Diversity

Part of ethics is going beyond the ordinary call to ensure inclusivity, accessibility, diversity of thought, and fairness. From a national security standpoint, diversity improves content moderation and community safety, particularly in hate speech identification and foreign language monitoring. Online platforms must embrace diversity, and a clear first step is through supporting employee resource groups and diverse recruitment initiatives at all levels of companies–from entry-level to senior management–with money and institutional clout. This is meant to provide alternative perspectives and to build out internal feedback channels for positive change. By bringing the views of diverse communities into the design process from

day one, services and products will more effectively take into account differing perspectives on ways in which services and products are used, including input on how they may be used in harmful ways and how those harms may be mitigated.

3) Ensure Respect for Digital Rights

To integrate these concepts on the ground, some of these efforts must develop best practices and training for employees in online platforms that can serve as a guiding north star in ethical design, operation, administration, and governance. Such training should include a signed commitment from employees to follow a Developers' Code of Conduct and from companies to adhere to the Information Governance Principles, in addition to respecting users' Digital Rights. *For further detail on these concepts, please see the illustrative Digital Bill of Rights and Developers' Code of Conduct discussions later in this Report.*

EMPOWERED PUBLIC

TASK FORCE RECOMMENDATION

All stakeholders, including government, platforms, community groups, academia, and civil society, have an obligation to educate and provide tools to online users so they are empowered to think critically, to advocate for their interests in the digital world, and to participate in democratic processes.

GOALS	POSSIBLE STEPS TO ENACTMENT	
Education	Locally-Focused Civic Education: K-12 and Adults	Support for Local Arts, Culture, and Journalism
Mobilization	Community Conversations to Set Online Norms	Engaging New Audiences with Workshops and Influencer Outreach
Agency	Interoperability	User Interface Adjustments

A new digital age offers immense possibilities for individuals, but only if we are properly prepared to manage its complexity. Under the current internet model, individuals' attention is treated as a product to sell, with the consumer but a means to the ends. New technologies, like blockchain for example, could shift the onus of security squarely onto the shoulders of individuals, with consequences both good and bad. With education from platforms about how their algorithms work, the public must prepare to assess the implications of new power dynamics in the digital landscape, so as not to be left vulnerable to future exploitation by narrow interests.

GOAL: The public needs 1) education to understand new technologies and their consequences, 2) effective mobilization to advocate on issues of public importance, and 3) agency over personal data and choices.

Individuals must actively grapple with the complexity and implications of their online existence. This is only possible with some education about the technologies themselves, the way they influence individual choice, and the motives of platforms and content producers. To safeguard the rights and interests of consumers, individuals must mobilize, in grassroots campaigns and otherwise, and take active steps to advocate with both policymakers and corporate leaders. Finally, individuals need agency to fully participate in and shape their experiences online. Micro-targeting and other funneling techniques by online platforms absorb users' attention, benefitting advertisers at the expense of individuals' time and autonomy.

While there are social goods that come out of these models, like free products, users need the freedom to choose these relationships, rather than being forced into acceptance by monopolistic realities.

RECOMMENDATION: All stakeholders, including government, platforms, community groups, academia, and civil society, have an obligation to educate and provide tools to online users so they are empowered to think critically, to advocate for their interests in the digital world, and to participate in democratic processes.

Democracy requires an engaged public to think critically about the rules and norms necessary for a healthy society, and this is true as much for digital society as it is for the real world. All stakeholders should have an opportunity to participate in specifying these rules and norms, including developing and using tools to realize them.

1) Develop Civic Tools of Education to Ensure Greater Societal Understanding of Risks and Opportunities Presented by Online Participation

In the first order, stakeholders should develop, promote, and distribute tools that support civic education that promotes a healthy digital society. Civic education for a healthy digital society is most effective where there is greatest trust, likely at the local level. Local level education efforts can be in dialogue with national, and sometimes international conversations, about how to establish rules and norms and what tools work best under what circumstances. One of the (relatively few) benefits of the pandemic was greater acceptance of the use of video conferencing, which would somewhat offset the time and travel investments otherwise required to enact such a plan. To ensure quality and consistency however, local efforts should be ultimately guided by national-level frameworks. Moreover, civic education works best when it includes and empowers diverse communities, especially since marginalized communities are the largest targets for online abuse. Part of this diversity are advocacy groups and government agencies that protect consumers and support accessibility.

From a content perspective, civic education must offer politically neutral understanding and promote critical thought while furnishing a baseline-level understanding of technology. Educational efforts should cover, with ample input from all stakeholders including across the political spectrum: digital literacy, privacy and security consciousness, tech ethics, digital readiness, mitigating digital risks, and mental health management. Critical thought, in this context the constant questioning of the content, algorithms, and other systemic structures of digital society, is therefore an important element of public empowerment alongside general understanding of technology and its consequences. Such critical thinking regarding the digital world should be part of widespread civic education.

Educational content and materials should be provided at the state and local levels to students as young as kindergarten, and funding for these efforts may be supplemented through grants made available at the federal level. In addition, congressional funding and expanded mandates of government-funded entities with public education and information functions like PBS, universities, and state boards of education, can offer such education to the broader adult public. Other promising avenues for education include local government-sponsored seminars, wherein local leaders could discuss how to identify mis/disinformation online, the harms caused by toxic and uncivil social media environments, and safety measures to protect children.

State and local governments, foundations, companies, and individuals must also invest in local arts and culture organizations to run exhibits that combat online mis/disinformation through education, and other community dialogues to build consensus around social norms that apply on and offline. Historical and even current models for such action abound. Elks lodges community events and local museum dis-

plays are two. These groups must also come together to support local journalism to build a shared base of trusted information and local connection. The resulting community cohesion can foster understanding and spark collective advocacy efforts if community members decide they want particular changes.

2) Mobilize Democratic Tools to Protect Users and Society from Potential Harms

An empowered public requires a democratic voice in digital society, which can be accomplished through means remarkably similar to those of the physical world. Grassroots campaigns can leverage the convening power of such organizations to pressure both platforms and government on issues like increasing user ownership capabilities on platforms, adopting a Bill of Digital Rights, improving data transparency for academics, accessibility and inclusion, and other key issues. Building campaigns in any domain requires a high degree of social cohesion, which could be achieved in part through in-person conversations among diverse community contacts. At the conversations, local communities would establish a "social contract" around behavior on local social media message boards and sites. The use of local social norming can reinforce civil online interactions and create new outlets for online dispute resolution outside of the platforms themselves.

In addition to promoting local engagement, it will be critical to bring together parties who don't normally communicate, and to convince a wide swath of society to participate and be heard. For example, fiction workshops by nonprofits in communities could invite youth to write about the types of new technology they want to see, and connect them with startups looking to innovate in rural settings, as a way to co-create business models around new technology. As another example, a national "coffee house" initiative, based out of local businesses, public libraries, and perhaps major cafe chains, could create the modern version of community dialogue centers. As well, a national foundation or advocacy group could convene a diverse cohort of social media literate young people to educate and mobilize the public to demand new, responsible solutions to clean up the privacy, security, and information ecosystems. To be successful, mobilization must be both local and inclusive.

3) Give Users Agency Over their Online Experiences

The final component to user empowerment is that they must have the opportunity and the ability to participate in shaping the contours of their personal online experiences. Ideally, they need to control their own data, make choices unencumbered by platform manipulation or subterfuge, have the freedom to move seamlessly between platforms, and access tools that give them more control over different aspects of their online expressions. The ability to "vote with your feet" by leaving platforms that do not meet users' needs or expectations is a critical component of shaping platform practices and policies; however, portability of information that may have been amassed on one platform and not transferable to another prevents users from exercising this option.

An interesting first step in this direction would be an embrace of interoperability standards, wherein consumer rights advocates and platforms would engage in discussions about priorities for users when developing interoperability standards and best practices for offering users more control over their profiles, content creation, and personal data.

At a platform specific level, users would benefit from a wider variety of tools to give them insights "behind the curtain" of their own internet experiences, including a more over ability to shape the content they see, why that content is presented to them, and who they are interacting with via content or directly. Enhanced user tools might include a button or flag to easily communicate to their networks their personal levels of assuredness about the credibility of the content they are sharing. Some form of interoperable identity

infrastructure, to standardize across platforms certain information about individual users, could also be explored, though mechanisms to protect vulnerable groups like dissidents or children would need inclusion. In addition, community groups could dialogue and generate new best practices ideas for user interface hurdles to accessing questionable content. For example, they could discuss forcing multiple click-throughs to access longform articles or removing automatic hyperlinks for sites deemed to provide large volumes of mis/disinformation; not automatically including article and headline previews with user posts; giving users the ability to remove "like/dislike" or "retweet" buttons; or requiring a checkmark that "I read this" before posting. While actual solutions may vary by platform, creating mechanisms for user participation in shaping their own experiences in digital society is fundamental to the thriving of democratic principles online.

C. Other Steps Towards a Healthy Digital Ecosystem

In addition to the Task Force's three primary recommendations, members analyzed over 80 additional ideas developed over the course of Task Force deliberations and stakeholder interviews to promote a healthy digital ecosystem. Here is a sampling of some of the ideas that received some, but not universal, support. While some remained exceptionally controversial among Task Force members, we include them in this Report with the hope that they will increase the breadth of future dialogue and, in the course of further debate, perhaps generate new approaches to the current risks posed by next generation social media.

STANDARDIZED CONSUMER CREDIT SCORING SYSTEM

Currently, consumers have no easy way to discern credible sources from those that consistently spread thirdhand, false information, including from authoritarian state-supported and amplified propaganda. One way to tackle the mis/disinformation deluge might be to create an "originality index" that prioritizes accounts in search algorithms and labels them based on the volume of mis/disinformation they create, promote, and share. From a structural perspective, the index could initially draw on the voluntary industry model used by the Codes of Practice in the EU and Australia. The index would serve two purposes, giving users the ability to see the quality of information they consume from others and providing a "check" for users before they repost from sources known to spread propaganda or falsehoods.

As the metaverse evolves and avatars become increasingly personal, the index could extend the existing American Credit Score system to standardize digital responsibility and ethical standards across platforms. There may also be a need to compare virtual with physical behaviors, cross-referencing metaverse behavior with airline "No Fly" lists, for instance. Given the metaverse's likely role as a new virtual public square of sorts, such systems should offer public accountability and appeals processes, potentially with private citizens invited to serve on screening panels under a type of "citizen jury" system. With careful attention to bias factors, some form of standardized credibility score might offer unique benefits as virtual technologies evolve.

AMENDING EXISTING LAWS TO KEEP PACE

A key theme throughout the Task Force's discussions, and particularly future threat simulations, was the inadequacy of current legal frameworks to address some of the novel concerns that arise as these new technologies become widespread. In the near future, a federal work group could recommend amendments to consumer protection laws, criminal laws, and regulations at both the federal and state level to keep pace.

As a starting point for such exploration, consumer law could expand to cover algorithmic bias under anti-discrimination laws and psychological harms under consumer product safety issues. New laws could

create private rights of action or be enforceable by existing or new regulatory agencies. With novel fact patterns slowly emerging, tweaks to criminal law definitions of threat and specific harms might improve applications to the VR context. Federal rulemaking to define what constitutes data abuse and exploitation in decentralized or virtual environments and to stipulate compliance and enforcement might be another preliminary executive branch step in this space. Updates to existing regulatory definitions and rules for executive agencies to address emerging threats might include broadening CFIUS purview, increasing export controls industry coverage, clarifying SEC disclosure rules on DeFi, instructing the FTC to publish Codes of Conduct for tech companies, or augmenting IRS authorities. The diversity of these examples demonstrate the breadth of implications a virtual world might have for our laws, and the need for a comprehensive legal strategy to prepare for them.

CARROT AND STICK ENFORCEMENT

The fundamental misalignment of incentives for some companies vis a vis consumer interests may require more direct action. There are both voluntary and mandatory ways to address this problem, as with the internally enforced industry standards and through taxation or government enforcement mechanisms mentioned under the Responsible Platforms recommendation above.

To take a private sector standards effort further, perhaps using the previously mentioned ESIG model, the government (in close coordination with private industry), at a later stage, may consider offering incentives to encourage investors to promote ESIG principles. Incentives might include directly funding anti-surveillance or other democracy-technology business models, tax breaks for individuals and funds to invest in ESIG solutions, funds for state and local governments to invest in ESIG solutions, or creating a new category of "accredited investors and qualified purchasers" that must meet ESIG principles.

Financial support for such programs could come from a levy of 1% or more on targeted advertising that tracks, combines demographic and psychographic data to generate user profiles.[190] Based on ideas raised from a number of sources, including media activist organization Free Press and noted economist Paul Romer, a tariff at 1% alone would bring in between $1-2 billion annually to support the incentives outlined.[191] Aside from funding incentives, this tariff could also support the study of the effects of social media on individuals and society at large.[192] This is an important proposition given the addictive effects of social media and their role in increased political polarization.[193]

Our intentions are to push our incentive structure systems to encourage healthy and quality ecosystems, while spurring a wave of innovations across a whole of society approach that can scale this. That includes carrots and sticks and while we would prefer the markets and private industry to handle this on their own, additional taxation would likely be necessary to support this proposal at scale. At the same time, such additional taxation could also act as a deterrent for irresponsible investors and force public disclosure of investors whose investments or practices do not further ESIG principles. For example, a new tax on funds and fund managers might penalize those that either invest or receive money from non-ESIG committed countries and limited partners. Similarly, for investors whose limited partners come from adversarial or non-democratic regimes, there could be an interest tax. Finally, there should be a restriction and reduction of federal funding for states that invest in business models that do not promote ESIG principles.[194] Finally, we need new sales tax breaks and penalties, as well as other incentive programs, to reward consumers who purchase products by companies that support ESIG principles. Healthy digital media ecosystems can only thrive where incentives are properly aligned to foster that. A concentrated emphasis on promoting ESIG principles is a potentially useful first step.

D. Tools for Implementation

Members of the Task Force undertook a first pass at the key tools that the recommendations highlighted as necessary, creating sample documents that express the democratic principles in different forms and can serve as the jumping off point for the realization of those ideas. The following three tools correspond to the Responsible Platforms recommendations.

SAMPLE DIGITAL BILL OF RIGHTS

As virtual technologies evolve, users will need protections from harms that don't fall neatly into existing frameworks. Accordingly, the Task Force highlighted the necessity of establishing new foundational digital rights to guide a healthy digital world. Here is a preview of potential rights that could be included to ensure that individuals can engage in the digital world. They are drawn from the considerations raised through the Task Force's lengthy discussions. In many ways they are a companion document to the Democratic Principles highlighted earlier, a distillation of the individual protections that flow naturally from those principles that must be considered by all stakeholders addressing the internet's new challenges.

i. Individual Rights

RIGHT TO IDENTITY: Individuals have the right not to have their identity assumed for the purpose of engaging in fraudulent behavior or material misrepresentation.[195]

RIGHT TO BODILY AUTONOMY & INTEGRITY: Individuals have the right to protect themselves or otherwise be protected against unconsented interference with their body through external manipulation, such as haptic gaming suits, VR headsets, or sensors. Individuals have the right to not experience harm or unwanted touching of their physical body or their avatar.

RIGHT TO CONTROL DATA: Individuals have the right to control the collection, sale, transfer, and deletion of personal data, including:[196]

Data Transparency: Individuals have the right to know the truth about how user data-driven companies, platforms, and other private entities are using user-generated data. This includes the ability to obtain information about how the platforms are feeding information to users and handling users' own data, as well as a right to have publicly available and documented APIs that facilitate auditing, research, interoperability, and standardized access to digital platforms.

***Biometric Data*:** Individuals have the right to keep the measurements of their physiological characteristics private; public authorities may only retain biometric data under certain circumstances. The data of individuals that is gathered through brain or body scans cannot be used against them in legal or administrative proceedings. Biometric data includes, inter alia, pupil dilation, sweat responses, heart rates, and other indicators of brain and bodily activity.

***Data Portability*:** Individuals have the right to collect and transfer their personal data from one platform to another.

***Data Security*:** Individuals have the right to trust that data they provide to third party sources is protected against public intrusion and cyber threats.

***Express Consent*:** Individuals have the right to give initial, express, consent before being monitored, surveilled, or engaged in interactions by other users. Individuals have the right to prevent corporate entities and others from tracking or surveilling their movements online.

ii. Rights within the Public Square

RIGHT TO FREE ASSOCIATION: Individuals have the freedom to associate with others in the digital realm.

RIGHT TO VERIFICATION: Individuals have the right to know with whom they are interacting in the digital realm, whether their identity is masked, and whether the entity with which they are interacting is a person or not.[197]

RIGHT TO BLOCK: Private individuals have the right to foreclose metaverse interactions with another user for any reason, at any time.

RIGHT TO DUE PROCESS/RIGHT AGAINST ERASURE: Individuals have the right to notice, third party review, an opportunity to be heard, and an appellate process, prior to removal from a platform.

RIGHT TO THE PHYSICAL WORLD: Individuals have the right not to be forced into virtual reality. They have the right to live and obtain essential goods and services in the physical world. This might mean that platforms cannot provide a 100% virtual experience, or must support physical world channels, to engage in basic human activities like shopping for food, attending school, accessing government services, or other areas into which they might eventually venture.

iii. Participatory Rights

RIGHT TO INCLUSION IN DECISION MAKING: When governments or platforms make major decisions that affect the direction of the internet and virtual worlds, the public has a right to be consulted and included in that decision making.[198]

RIGHT AGAINST DISCRIMINATION: Companies will not make decisions that will discriminate against individuals on the basis of race, color, religion, sex, national origin, disability, age, sexuality, or any other protected status.

RIGHT TO PROTECTION OF VULNERABLE PEOPLE/COMMUNITIES: Parents and guardians have the right to implement measures they consider imperative for the protection of and best interest of vulnerable people under their care. Government retains similar rights where protection of the citizenry is at stake.

RIGHT TO ACCESSIBILITY: All individuals shall have access to the technology and platforms needed to fully participate in virtual worlds whether it is for education, entertainment or other purposes, regardless of socioeconomic or other status. To enable persons with disabilities to independently access and participate in all aspects of digital life, appropriate measures will be taken to ensure equal access to the Internet, communications technologies and systems.

RIGHT TO COMMUNAL SAFETY: Communities have a right to establish and enforce norms for appropriate behavior within their online forums, similar to how restaurants may refuse service to those acting in ways outside the scope of their accepted standards for decorum.

iv. Algorithmic Inclusion and Transparency

RIGHT TO ALGORITHMIC TRANSPARENCY: Individuals, researchers, and others have the right to explanations of any algorithms governing data collection and distribution and the right to study and make public their findings on the logic, significance, and impact of algorithms and automated decision-making.

RIGHT TO FINANCIAL & BUSINESS MODEL TRANSPARENCY: Individuals and the public have a right to obtain information about company pricing, revenue, and profit generated on private data across the digital sphere. Individuals have a right to information about personal data supply chain instantiations.

RIGHT TO REPRESENTATION: In mass data sets used to train algorithms, people of all races, religions, disability status, genders, and other protected classes have a right to be represented to try to minimize algorithmic bias.

v. Tools to Navigate the Public Square Safely

RIGHT TO DIGITAL PUBLIC EDUCATION: Individuals have the right to public education that will equip them to navigate the digital realm in a safe and secure way, as well as evaluate the consequences of adopting new technology or sharing their personal data online.

RIGHT TO DISCONNECT: All hardware will be built to offer individuals an immediate disconnection from electronic devices and online platforms, at will, in order to remove themselves from a harmful situation.

RIGHT TO NOTIFICATION: Individuals have the right to be alerted if threats or actions targeting their virtual or physical presence are made in a particular virtual space.

RIGHT TO BE FREE FROM DECEPTIVE COMMERCE: Individuals have the right to be protected from unfair, deceptive and fraudulent products and services. Companies or platforms who sell user data or otherwise make profit from user data must treat users fairly and honestly, putting user interests first.

vi. Right to Enforcement

RIGHT TO ENFORCEMENT INFORMATION: The public has the right to information about steps companies are taking to adopt, adhere to, and enforce these Digital Rights. Public and private grant makers and investors have a right to require the adoption of these Digital Rights or information about the steps companies are taking to adopt and enforce them as a condition of investment.

DRAFT DEVELOPERS' CODE OF CONDUCT

The Developers' Code of Conduct, modeled on the Hippocratic Oath undertaken by medical professionals, is meant for online platforms and emerging technology companies to consider their broader societal obligations. Building out industry certifications, like those adopted by medical personnel, mechanical engineers, lawyers, and other professions will require significant further discussion, but companies, educational programs, and other stakeholders can adopt ethics trainings and codes of conduct to orient developers now towards the greater societal good. Such a code could contain the following concepts:[199]

- ☐ I pledge to design projects with public safety, human rights, democracy, and the good of society in mind.
- ☐ I pledge to refrain from intentionally causing harm to my enterprise, society, or others, in service of my own personal gain.
- ☐ I pledge to make the fruits of my efforts accessible to all people, regardless of race, sex, disability, or other status.
- ☐ I pledge to architect my products to provide data and functionality through publicly available and documented APIs and service interface calls that will be externalizable.
- ☐ I pledge to develop products who's user experience provides less friction and better ease of use in every iteration.
- ☐ When confronting a problem with uncertain impacts, I will seek input from others, including those who might face disproportionate impact, and consider the risks before proceeding and throughout.
- ☐ I will respect the privacy and sanctity of individuals, taking care to ensure the security of their personal data and only using it with their approval.
- ☐ I will aim for transparency and share my knowledge as much as possible, to help advance scientific knowledge and to open that information to all who come after me.
- ☐ Most importantly, I will remember that technological innovation is meant to serve the good of humanity, and I will strive to contribute to that progress.

INFORMATION GOVERNANCE PRINCIPLES

The following Information Governance Principles could form the basis for ethical standards for industry self-regulation, either standalone or as an addition to the existing model of ESG principles in the investing world. They are meant as a guide to support more concrete metrics for companies to implement, and, above all else, to support democracy. They can also be used in conjunction with similar efforts in this area by other organizations.[200]

INFORMATION INTEGRITY: Provide reliable, contextualized content to users.

DEMOCRATIC NORMS: Create channels to include the public in decision making with regard to major decisions that affect the direction of the internet and virtual worlds.

INTELLECTUAL DIVERSITY: Allow a wide variety of perspectives to flourish, limit the ideological funneling of content to users without their express consent.

PRIVACY: Protect user data, including access history and sensitive personal information, from cyberattacks and deanonymization.

UNIVERSAL ACCESSIBILITY: Support access to internet services via a variety of mechanisms to accommodate for socioeconomic, racial, religious, disability, and other statuses.

SPECIAL PROTECTIONS: Ensure that users with heightened risk profiles are considered and protected, whether they are minors, the developmentally disabled, political dissidents, or otherwise.

DATA OWNERSHIP: Help users control and understand their data, including data collection and usage practices, and create pathways for them to monetize their own data or carry it across different platforms.

OPENNESS: Share anonymized data with and support researchers, and educate the public about commercial practices that implicate their privacy, access to information, and other aspects of their online lives to inform public discourse.

FAIRNESS: Apply Terms of Service and platform standards evenly across all users, enforce penalties for harassment and threats, and, where possible, offer services for victims to be made whole.

VI. Our Approach

A. Who We Are

Georgetown Law Center on National Security *National Security Crisis Law Simulation Invitational*, 2018

The Georgetown Law Center on National Security is the nation's premier academic center on national security law, conducting cutting edge research and training the next generation of lawyers through our JD and LLM national security law programs. Anchored by the strongest and most diverse national security faculty in the country, the Center is at the forefront of the national security conversation. It operates with a "NatSec 360" perspective, a holistic and multi-disciplinary approach to identifying and addressing some of the most pressing concerns in national security law and policy.

The Center recently expanded its work as a think/do tank, connecting research to real world problems. Our marquee initiative is the launch of our Incubators: problem solving labs dedicated to finding and implementing novel, cross-sector solutions to complex security problems at the intersection of law, policy,

and society. To support the Incubators, the Center is constructing an innovation methodology that builds on design thinking, creative problem solving, complexity theory, organizational behavior, change management and related fields. Our goal is to help to protect the security, well-being, and rights of people at home and in the world.

The four initial Incubators focus on new and emerging technology (NatSec Tech); international peace and security (NatSec Humanity), natural security (NatSec Nature), and national security institutions (NatSec Institutions). This project is the first deep dive launched by the NatSec Tech Incubator.

B. Why Think Differently

National security threats to the United States are evolving rapidly, and the American national security apparatus must pivot to meet the moment. The National Security Act of 1947 shaped a governance landscape to address discrete, physical threats from nation states. Our enemies were easily identified and defined, as were their objectives, within a broader great power competition. Competition continues, albeit with new major players and alliances, but it looks different. The greatest existential threats to US national security have changed.

One such threat arises from one of our most important strengths: technology. Emerging technology allows us to do everything from create new life forms to construct killer robots. Modern social media companies capture what you read, what you believe, and what you do (and with whom). Using predictive algorithms, they can anticipate your friendships, your purchases, and which candidate you will support. Like their online retail counterparts, they have access to billions of records, creating risks of mass surveillance, microtargeting, and identity theft. Simultaneously, innovations in social network analytics and algorithmic sciences have radically expanded the scope of what can be done with the information gleaned.

Traditional national security actors, in many ways, stand on the periphery. The role of private industry in emerging technologies is dominant and expanding, and the "classified side" no longer has a monopoly on cutting-edge technology or data/metadata.[201] Massive investments by the world's largest companies leave the US government behind in certain critical areas. While companies can offer significant benefits to the public, their interests are not the public's. They are not the government, and the private sector's negative effects on our democratic society are often an afterthought. Our adversaries' ability to steal or abuse private sector technologies complicates the equation further. The US government must grapple with this shift in power — how to protect the public when some of the most dangerous potential weapons are no longer under government control–and are not traditional weapons at all.

The lines between security, law, and technology have never been less clear, yet so important. We are not Luddites, and the potential benefits of these technologies cannot be overstated. The promise of this new world requires our national security leadership to venture into new arenas, with new considerations at play from other corners of our society. Building a thriving, safe, and democratic society is not easy. The role of the national security apparatus must evolve with the technology and the times. In this environment, it is critical to think differently about what new technologies are coming down the pipeline, how they will change society, and how, if at all, the national security community should pivot to meet these changes.

C. Project Design

Inspired by design thinking and other theories on innovation, our research methodology was far broader than a traditional national security project. Over the course of 18 months, we convened a consortium of scholars conducting original research; reviewed hundreds of relevant studies, patent applications, and

previous Task Force publications; interviewed almost 100 individuals from a variety of backgrounds; and engaged our Task Force members in four major workshops, as well as numerous small group meetings. Our goal was to gain breadth and depth in these topics. From a seemingly infinite pool of emerging digital technologies, we culled a list of some of the most critical innovations that we anticipate will play a key role in the future. We prioritized those with the most solid current technical foundations, those gaining the most mainstream use traction, and those that have most captured the public imagination.

Ultimately, we settled on five categories of technologies to explore: extended realities, artificial intelligence, Web3, infrastructure challenges, and biodata collection. We interviewed technical experts in an attempt to separate the technological realities from Silicon Valley's oft-discussed hype. Every step of the way, we consulted representatives of the major social media platforms. From there, we sought to understand the current pace of innovation, and how these technologies are likely to interact over time.

Predicting the future is an inherently dicey proposition. To ground our work, we developed a number of highly detailed future scenarios around the major technologies and their national security-related vulnerabilities.[202]

After debating current gaps in our security frameworks for addressing these scenarios, the Task Force developed a streamlined set of primary harms to address, the most salient democratic principles to guide solutions, and a more concrete set of criteria for evaluating potential solutions. Collectively, these concepts undergirded a novel framework for considering the unique national security concerns posed by the internet's emerging technologies. Ultimately, they were used both as part of the endorsement process for concrete next steps. They are offered here in the Roadmap to a Healthy Digital World to help subsequent efforts by other organizations that can benefit from these first principles.

We developed and applied a novel framework to a deeply complex, evolving ecosystem with significant national security implications. In our increasingly interconnected world, where knowledge and advanced technology are available to every global citizen, not just nation states or well-funded entities, the definition of a "national security issue" must be expanded beyond our current post-World War II frameworks. We hope that our model can serve as a jumping off point for future thinking on similarly pressing issues.

D. Task Force Members

LAURA K. DONOHUE

Donohue is the Chair of the Social Media Governance Task Force, Professor of Law at Georgetown Law, and Director of Georgetown's Center on National Security as well as the Center on Privacy and Technology. She writes on political theory, public law, constitutional law, foreign intelligence, federal courts, national security, and legal history. Her work on new and emerging technologies centers on next generation social media, biometric identification and manipulation, augmented and virtual reality, artificial intelligence, and drones.

MATT ABRAMS

Abrams is a technologist, investor, advisor, speaker, and outdoor adventurer who inspires startup founders and C-level executives to think bigger and bolder. His expertise and focus is in: Enterprise Data & Analytics, Artificial Intelligence (AI) & Machine Learning, Information Quality & Integrity, Security, and Healthcare. He has spent over 25 years in the Enterprise software industry working across various Government, Healthcare, Startups, Enterprises and Venture Capital Funds and organizations.

GERRIN T. ALEXANDER

Alexander is a Senior Opinion Editor for the Chicago Thinker. As a 2021 graduate from the University of Chicago, Gerrin holds degrees in Political Science and Public Policy. Much of her political interest stems from research concerning the intersection of faith and politics within the African American community. She loves longboarding, cooking, hanging with her family, watching anime, reading manga, and traveling.

LEONARD BAILEY

Bailey is Head of Computer Crime and Intellectual Property Section's (CCIPS) Cybersecurity Unit and Special Counsel for National Security in the Department of Justice's (DOJ) Criminal Division. He joined DOJ's Terrorism and Violent Crime Section in 1991. In the late 1990's, he served as Special Counsel and Special Investigative Counsel to DOJ's Inspector General and supervised sensitive investigations of Department officials and programs.

SHARON BRADFORD FRANKLIN*

Sharon Bradford Franklin is Chair of the Privacy and Civil Liberties Oversight Board. Prior to her appointment as Chair, Ms. Franklin served as Co-Director of the Security and Surveillance Project at the Center for Democracy & Technology (CDT), leading advocacy on a broad range of issues involving surveillance, cybersecurity, encryption, civil liberties, and civil rights. Previously, she was the Policy Director for New America's Open Technology Institute (OTI), directing OTI's policy work on issues including cybersecurity, encryption, freedom of expression online, government surveillance, privacy, and platform accountability. From 2013 through 2017, Ms. Franklin served as Executive Director of the Privacy and Civil Liberties Oversight Board. She supervised and directed the PCLOB's staff in reviewing federal counterterrorism activities in support of the Board's mission to ensure that such programs include appropriate safeguards for privacy and civil liberties.

**Participated in dialogue with the Task Force but does not take any position on the Report and recommendations.*

WHITNEY KIMBALL COE

Coe is a vice president and Director of National Programs for the Center for Rural Strategies. She directs the work of the National Rural Assembly, a program that brings together rural leaders and advocates from every region with national public- interest organizations, funders, and policymakers in ways that inform public policy and private investment in rural people and places.

DOOWAN LEE

Lee is the CEO and cofounder of VAST-OSINT. With VAST-OSINT, he builds automated data analytic tools to detect and expose the origin of disinformation and how it propagates across the media ecosystem. He has published extensively on how to combat both state-sponsored and extremist influence campaigns.

JUDGE MARGARET MCKEOWN*

McKeown was appointed to the United States Court of Appeals for the Ninth Circuit in 1998. She graduated from Georgetown University Law Center in 1975 and holds an honorary degree from Georgetown University. She has published and lectured throughout the world on intellectual property, international law, ethics, and constitutional law and has participated in numerous rule of law initiatives with judges and lawyers.

**Participated in dialogue with the Task Force but does not take any position on the Report and recommendations.*

SAIPH SAVAGE

Savage is an Assistant Professor at Northeastern University and co-Director of the Civic Innovation Lab at the National Autonomous University of Mexico (UNAM). For her civic tech research, Dr. Savage was named one of the 35 Innovators under 35 by the MIT Technology Review where she focuses on organizing citizen crowds to address critical problems in society.

AMANDA SHANOR

Shanor is an Assistant Professor at the Wharton School at the University of Pennsylvania, where her scholarship focuses on constitutional law, and in particular the intersection of the First Amendment and economic life. Prior to joining the academy, Shanor was a practicing lawyer in the National Legal Department of the American Civil Liberties Union.

CONGRESSWOMAN LORI TRAHAN

Trahan proudly serves Massachusetts' Third District. Growing up in a working-class family in Lowell, Massachusetts, Lori learned the principles of sacrifice, hard work, and grit. The first in her family to graduate college, Lori earned a scholarship to play Division 1 volleyball at Georgetown University. After college, she joined former Congressman Marty Meehan's staff, working her way up to Chief of Staff. After serving Massachusetts for nearly ten years, Lori moved to the private sector as the only female executive at a tech company and later a co-founder of a women- owned and -operated consulting firm focused on elevating women to leadership positions.

IRENE S. WU

Wu teaches in Georgetown University's Communications, Culture and Technology, and is also a senior economist at the US Federal Communications Commission. She is author of the books *From Iron Fist to Invisible Hand: the Uneven Path of Telecom Reform in China, Forging Trust Communities: How Technology Changes Politics,* and several articles on measuring soft power in international relations. She participated in her personal capacity only, and her work does not reflect the views of the Federal Communications Commission, its members or its staff.

An expert from a major social media platform also participated in their personal capacity, made substantive contributions at each Task Force meeting, and helped to shape the recommendations. We are grateful for their insights and technical assistance.

VII. Conclusion

The emerging social media threats discussed in this Report are capable of causing damage that is far-ranging and insidious. The most concerning threat is to American democracy. At the same time, squelching social media is both futile and counterproductive.

Social media is an integral part of societal fabric and its role continues to grow across new social, professional, and political domains. In addressing the threats of social media and similar threats raised by rapidly emerging technologies, the national security community must strike a balance. Novel solutions must harness tools from outside the traditional national security sphere, and democratic principles must guide these efforts to an ultimate goal of fostering democracy and democratic processes.

The social media paradox magnifies the ongoing struggle to preserve liberty and underscores the role of non-government actors in protecting against potential threats to the United States. Yet, this work could not be more urgent, as new emerging technologies raise graver societal concerns at a pace the government cannot currently match. When assessing the likely nature of future national security threats, social media has become the proverbial canary in the coal mine.

Acknowledgments

I am grateful to the Public Interest Technology University Network (PIT-UN), for generously providing funding for this project. Anna Cave, the Executive Director of the Center on National Security, helped to design, coordinate, and execute it. The Report benefited from the deliberations of the Social Media Research Colloquium, which convened weekly January through June 2021. That group included Monique-Agnes Ladeji, Leonard Bailey, Lauren Cherry, Gunjan Chawla, Dr. Beba Cibralic, Professor Julie Cohen, Jordan J. Foley, Dr. Mark Hanin, Kristen Logan, Professor Amanda Shanor, and Shervin Taheran. Starting in June 2021, Matthew Ivey and Andrea Woods stepped in to help shape the Task Force. Dawan Stanford and his colleagues at Fluid Hive, as well as Daniel Yi, Senior Counsel for Legal Innovation at the U.S. Department of Justice, helped us to apply design thinking to the process.

I am also grateful to our Task Force members, who took precious time to attend numerous meetings over the course of a year, provided comments on the documents, and contributed their formidable knowledge to the discussions. Jenny Reich coordinated a number of research projects, undertook dozens of interviews of key stakeholders, and helped to develop scenarios and to draft the final Report. The Center's research assistants, Sophie Chen, Manasa Chinni, Omar Haddad, Anna-Alexia Kotsakis, Yaegy Park, Ozoda Usmanova, and Patience Williams-Cook, made further helpful contributions. In addition, Mark Chandler, a Senior Fellow with the Center, and Peter Neal, our Center Associate, offered valuable comments and insights.

Finally, I extend my gratitude to Dean William Treanor and to the leadership at Georgetown Law's Centers and Institutes, particularly Professor Rosa Brooks and Amy Gillies, who have provided steadfast support for the Center and helped us to launch the Incubators and their associated projects. It is much appreciated.

Prof. Laura K. Donohue
Director, Center on National Security
Georgetown Law

Endnotes

[1] Julian Hopkins, *How to Define Social Media – An Academic Summary*' Julian Hopkins Phd (Oct. 19, 2017), http://julianhopkins.com/how-to-define-social-media-an-academic-summary/; Jonathan A. Obar and Steven S. Wildman, *Social Media Definition and the Governance Challenge – An Introduction to the Special Issue*, **Quello Ctr. Working Paper** (2015), https://www.ssrn.com/abstract=2663153.

[2] One of the most prominent reports is the one issued by the Aspen Institute's Commission on Information Disorder. **Aspen Digital, Final Report, Commission on Information Disorder** (Aspen Institute, 2021), *accessible at* https://www.aspeninstitute.org/publications/commission-on-information-disorder-final-report/. We also found the following three reports on the international disinformation landscape particularly salient: **Andrea Carson, Fighting Fake News - A Study of Online Misinformation Regulation in the Asia Pacific** (La Trobe University, 2021), accessible at https://opal.latrobe.edu.au/articles/report/Fighting_Fake_News_A_Study_of_Online_Misinformation_Regulation_in_the_Asia_Pacific/14038340/1; **Olga Robinson, Alistair Coleman, and Shayan Sardarizadeh, A Report of Anti-Disinformation Initiatives** (Oxford Technology & Elections Commission, 2019), *accessible at* https://oxtec.oii.ox.ac.uk/wp-content/uploads/sites/115/2019/08/OxTEC-Anti-Disinformation-Initiatives-1.pdf; **Alina Polyakova and Chris Meserole, Exporting Digital Authoritarianism: The Russian and Chinese Models** (Brookings, 2019), *accessible at* https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf.

[3] Julian Hopkins, *How to Define Social Media – An Academic Summary*, Julian Hopkins Phd (Oct. 19, 2017), http://julianhopkins.com/how-to-define-social-media-an-academic-summary/; Jonathan A. Obar and Steven S. Wildman, *Social Media Definition and the Governance Challenge – An Introduction to the Special Issue*, **Quello Ctr. Working Paper** (2015), https://www.ssrn.com/abstract=2663153.

[4] Maria Alessandra Golino, *Algorithms in Social Media Platforms*, **Inst. for Internet and the Just Society** (Apr. 24, 2021), https://www.internetjustsociety.org/algorithms-in-social-media-platforms.

[5] Kokil Jaidka, Alvin Zhou, Yphtach Lelkes, Jana Egelhofer, and Sophie Lecheler, *Beyond Anonymity: Network Affordances, Under Deindividuation, Improve Social Media Discussion Quality,* **27 Jof Computer-Mediated Comm.** (2021), *accessible at* https://academic.oup.com/jcmc/article/27/1/zmab019/6427305; Aaron Smith, *Why Americans use social media*, **Pew Res.** (Nov. 15, 2011), https://www.pewresearch.org/internet/2011/11/15/why-americans-use-social-media/; Three Reasons Why Gaming and Social Media Go Hand in Hand, **NerdLeaks** (May 17, 2022), https://nerdleaks.com/videogames/three-reasons-why-gaming-and-social-media-go-hand-in-hand/.

[6] Beth Simone Noveck, James Button, Dane Gambrell, Lex Paulson, Paolo Spada, and Lakshminarayanan Subramanian, *The Power of Virtual Communities*, **The Gov Lab** (February 2021), https://virtual-communities.thegovlab.org/files/DTR_report_en_EN.pdf; Chris Beer, *The Rise of Online Communities*, **GWI** (Jan. 7, 2020), https://blog.gwi.com/chart-of-the-week/online-communities/.

[7] *Online communities and social communities: a primer*, **i-Scoop** (last visited Oct. 24, 2022)' https://www.i-scoop.eu/online-communities-social-communities-primer/.

[8] Chris Beer, *The Rise of Online Communities*, **GWI** (Jan. 7, 2020)' https://blog.gwi.com/chart-of-the-week/online-communities/.

[9] Todd Bishop, *Microsoft Teams surpasses 270M monthly active users, as growth slows from early days of pandemic*' **GeekWire** (Jan. 25, 2022), https://www.geekwire.com/2022/microsoft-teams-surpasses-270m-monthly-active-users-as-growth-slows-from-early-days-of-pandemic/; Tom Warren, *Microsoft is launching a Facebook rip-off inside Teams*, **The Verge** (July 19, 2022), https://www.theverge.com/2022/7/19/23268187/microsoft-viva-engage-facebook-work-yammer.

[10] Ellie House, *FinTok: how TikTok is helping young people use cash wisely*, The Guardian (July 10, 2021), https://www.theguardian.com/money/2021/jul/10/fintok-how-tiktok-is-helping-young-people-use-cash-wisely; *TikTok For Finance: The Rise Of Fintech & 'Fin-fluencers,'* **Fanbytes** (last visited Oct. 24, 2022), https://fanbytes.co.uk/fintech-influencers-tiktok/.

[11] *Social Investing*, **Etoro** (last visited Oct. 24, 2022), https://www.etoro.com/en-us/trading/social/.

[12] *Is Cryptocurrency the Future of Online Gaming?*, **The Daily Gazette** (last visited on Oct. 24, 2022), https://dailygazette.com/is-cryptocurrency-the-future-of-online-gaming/; Aliyah Kaye Cooke, *How Crypto is Evolving the Gaming Industry*, **Forum Pay** (Feb. 9, 2022), https://forumpay.com/blog/cryptoworld/how-crypto-is-evolving-the-gaming-industry; George Kaloudis, *Lightning Payments Come to Mobile Games, Fueling Bitcoin Adoption*, **CoinDesk** (Apr. 26, 2022), https://www.coindesk.com/layer2/paymentsweek/2022/04/26/lighting-payments-come-to-mobile-games-fueling-bitcoin-adoption/.

[13] Enrique Dans, *Has The Pandemic Launched Us Into The Age Of The Metaverse?*, **Forbes** (May 27, 2020)' https://www.forbes.com/sites/enriquedans/2020/05/27/has-the-pandemic-launched-us-into-the-age-of-the-metaverse/?sh=5e0e2f84a99d; Adam Simon, *How COVID-19 Is Leading Us to the Metaverse, Part One*, **IPG Media Lab** (May 14, 2020), https://medium.com/ipg-media-lab/part-1-how-covid-19-is-pushing-us-closer-to-the-metaverse-c76a46e21cd2.

[14] *Connect 2021: Our vision for the metaverse*, **Tech at Meta** (Oct. 28, 2021), https://tech.fb.com/ar-vr/2021/10/connect-2021-our-vision-for-the-metaverse/; Mark Purdy, *How the Metaverse Could Change Work*, **Harvard Bus. Rev.** (Apr. 5, 2022), https://hbr.org/2022/04/how-the-metaverse-could-change-work.

[15] Lik-Hang Lee, *All One Needs to Know about Metaverse: A Complete Survey on Technological Singularity, Virtual Ecosystem, and Research Agenda*, **arXiv** (2021), *accessible at* https://arxiv.org/abs/2110.05352; Jerameel Kevins, *Metaverse as a New Emerging Technology: An Interrogation of Opportunities and Legal Issues: Some Introspection*, **Colum. L. School Public L. & Legal Theory Res. Series** (2022), *accessible at* https://www.ssrn.com/abstract=4050898; Fei-Yue Wang, *MetaSocieties in Metaverse: MetaEconomics and MetaManagement for MetaEnterprises and MetaCities*, 9 **IEEE Trans. Comput. Soc. Syst.** 2 (2022), *accessible at* https://ieeexplore.ieee.org/document/9697993?signout=success.

[16] What America's largest technology firms are investing in, **The Economist** (Jan. 22, 2022), https://www.economist.com/briefing/2022/01/22/what-americas-largest-technology-firms-are-investing-in.

[17] *Id*.

[18] Amelia Fletcher, Big Tech: how can we promote competition in digital platform markets?, **Econ. Observ.** (June 16, 2022), https://www.economicsobservatory.com/big-tech-how-can-we-promote-competition-in-digital-platform-markets; Florian Ederer, Does Big Tech Gobble Up Competitors?, **Yale Insights** (Aug. 4, 2021), https://insights.som.yale.edu/insights/does-big-tech-gobble-up-competitors.

[19] Press Release, Federal Trade Commission, FTC Sues Facebook for Illegal Monopolization (Dec. 9, 2020), https://www.ftc.gov/news-events/news/press-releases/2020/12/ftc-sues-facebook-illegal-monopolization; Samriddha Sen, *Federal antitrust lawsuit filed against Google over Maps monopoly and Waze deal*, **Jurist** (Apr. 15, 2022), https://www.jurist.org/news/2022/04/federal-antitrust-lawsuit-filed-against-google-over-maps-monopoly-and-waze-deal/.

[20] H. Rep. No. 117-8, at 18 (2022).

[21] Michelle Odlum and Sunmoo Yoon, *What can we learn about the Ebola outbreak from tweets?*, 43 **American J. of Infection Control 563** (2015), *accessible at* https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4591071/; *How the Paris attacks unfolded on social media*, **BBC News** (Nov. 17, 2015), https://www.bbc.com/news/blogs-trending-34836214; John D. Sutter, *Theater shooting unfolds in real time on social media*, **CNN** (July 20, 2012), https://edition.cnn.com/2012/07/20/tech/social-media/colorado-shooting-social-media/index.html.

[22] Mason Walker and Katerina Eva Matsa, *News Consumption Across Social Media in 2021*, **Pew Res.** (Sept. 20, 2021), https://www.pewresearch.org/journalism/2021/09/20/news-consumption-across-social-media-in-2021/; Lars Willnat, David H. Weaver, and G. Cleveland Wilhoit, *The American Journalist in the Digital Age: How journalists and the public think about journalism in the United States*, 20 **Journalism Studies** 423 (2017), https://www.tandfonline.com/doi/abs/10.1080/1461670X.2017.1387071.

[23] Nic Newman et al., Reuters Institute Digital News Report 2021 (10th Ed., 2021), *accessible at* https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2021-06/Digital_News_Report_2021_FINAL.pdf; Eunae Yoo, *Evaluating information diffusion speed and its determinants in social media networks during humanitarian crises*, 45 **J. of Operations Mgmt.** 123 (2016), *accessible at* https://www.researchgate.net/publication/305112257_Evaluating_information_diffusion_speed_and_its_determinants_in_social_media_networks_during_humanitarian_crises.

[24] *Connect 2021: Our vision for the metaverse*, **Tech at Meta** (Oct. 28, 2021), https://tech.fb.com/ar-vr/2021/10/connect-2021-our-vision-for-the-metaverse/; Lisa M. Kruse, Dawn R. Norris, and Jonathan R. Flinchum, *Social Media as a Public Sphere? Politics on Social Media*, 59 **The Sociological Quarterly** 62 (2017), *accessible at* https://www.tandfonline.com/doi/abs/10.1080/00380253.2017.1383143; Riley Funk, *Social media crime reporting helpful to law enforcement*, **Yahoo!** (July 12, 2022), https://www.yahoo.com/now/social-media-crime-reporting-helpful-040100996.html?guccounter=1.

[25] Laura Silver, Christine Huang, and Kyle Taylor, *In Emerging Economies, Smartphone and Social Media Users Have Broader Social Networks*, **Pew Res.** (Aug. 22, 2019), https://www.pewresearch.org/internet/2019/08/22/in-emerging-economies-smartphone-and-social-media-users-have-broader-social-networks/.

[26] Russell Heimlich, Using Social Media to Keep in Touch, **Pew Res.** (Dec. 22, 2011), https://www.pewresearch.org/fact-tank/2011/12/22/using-social-media-to-keep-in-touch/.

[27] Lindsay H. Shaw and Larry M. Gant, *In Defense of the Internet: The Relationship between Internet Communication and Depression, Loneliness, Self-Esteem, and Perceived Social Support*, **5 CyberPsychology & Behavior** 157 (2002), *accessible at* https://www.researchgate.net/publication/11346056_In_Defense_of_the_Internet_The_Relationship_Between_Internet_Communication_and_Depression_Loneliness_Self-Esteem_and_Perceived_Social_Support; Fenne große Deters, and Matthias R. Mehl, *Does Posting Facebook Status Updates Increase or Decrease Loneliness? An Online Social Networking Experiment*, 4 **Soc. Psych. and Personality Sci.** 579 (2013), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3820167/; Philippa Collin, Kitty Rahilly, Dr. Ingrid Richardson, and Amanda Third, *The benefits of social networking services*, **Lit. Rev.** (2011), *accessible at* https://www.westernsydney.edu.au/__data/assets/pdf_file/0003/476337/The-Benefits-of-Social-Networking-Services.pdf.

[28] Laura Silver, Christine Huang, and Kyle Taylor, *In Emerging Economies, Smartphone and Social Media Users Have Broader Social Networks*, **Pew Res.** (Sept. 22, 2019), https://www.pewresearch.org/internet/2019/08/22/in-emerging-economies-smartphone-and-social-media-users-have-broader-social-networks/.

[29] Lucie Kvasničková Stanislavská, Ladislav Pilař, Klára Margarisová and Roman Kvasnička, *Corporate Social Responsibility and Social Media: Comparison between Developing and Developed Countries*, **12 Sustainability 5255** (2020), *accessible at* https://www.mdpi.com/2071-1050/12/13/5255.

[30] Daniel Victor, *Pepsi Pulls Ad Accused of Trivializing Black Lives Matter*, N.Y. Times (Apr. 5, 2017), https://www.nytimes.com/2017/04/05/business/kendall-jenner-pepsi-ad.html; Yogesh K. Dwivedi, Gerald Kelly, Marijin Janssen, Nripendra Rana, *Social Media: The Good, the Bad, and the Ugly*, 20 Info. Syst. Front. 419 (2018), *accessible at* https://www.researchgate.net/publication/323945347_Social_Media_The_Good_the_Bad_and_the_Ugly.

[31] Kashif Ahmad, Konstantin Pogorelov, Michael Alexander Riegler, and Nicola Conci, *Social media and satellites: Disaster event detection, linking and summarization*, 78 Multimedia Tools and Appl. 2837 (2019), *accessible at* https://www.researchgate.net/publication/324543355_Social_Media_and_Satellites_Disaster_event_detection_linking_and_summarization; Clay Shirky, T*he Political Power of Social Media: Technology, the Public Sphere, and Political Change*, 90 Foreign Affairs 28 (2011), *accessible at* https://faculty.cc.gatech.edu/~beki/cs4001/Shirky.pdf; Paul S. N. Lee, Clement Y. K. So, and Louis Leung, *Social media and Umbrella Movement: insurgent public sphere in formation*, 8 Chinese J. of Commun. 356 (2015), *accessible at* https://www.tandfonline.com/doi/full/10.1080/17544750.2015.1088874.

[32] Jesse Fox and Katie M. Warber, *Queer Identity Management and Political Self-Expression on Social Networking Sites: A Co-Cultural Approach to the Spiral of Silence: LGBT+ & SOCIAL NETWORKING SITES*, 65 J. Commun. 79 (2015), *accessible at* https://www.researchgate.net/publication/269877555_Queer_Identity_Management_and_Political_Self-Expression_on_Social_Networking_Sites_A_Co-Cultural_Approach_to_the_Spiral_of_Silence.

[33] Chia-chen Yang, Jiun-Yi Tsai, and Shuya Pan, *Discrimination and Well-Being Among Asians/Asian Americans During COVID-19: The Role of Social Media*, 23 Cyberpsychology, Behavior, and Social Networking 865 (2020), *accessible at* https://pubmed.ncbi.nlm.nih.gov/32762541/.

[34] Jared L. Johnson and Clark Callahan, *Minority Cultures and Social Media: Magnifying Garifuna*, 42 **J. of Intercultural Commun. Res.** 319 (2013), accessible at https://www.tandfonline.com/doi/abs/10.1080/17475759.2013.842608; Clark Callahan, *Snapchat Usage Among Minority Populations*, 18 **J. of Media and Religion** 1 (2019), *accessible at* https://www.tandfonline.com/doi/abs/10.1080/15348423.2019.1639404.

[35] Joseph Jerome and Jeremy Greenberg, *Augmented Reality + Virtual Reality*, **Future of Privacy Forum** (Apr. 2021), https://fpf.org/wp-content/uploads/2021/04/FPF-ARVR-Report-4.16.21-Digital.pdf.

[36] *Id*.

[37] Paul Milgram and Fumio Kishino, *A Taxonomy of Mixed Reality Visual Displays*, 77 **IEICE Transactions on Info. Sys.** 1321 (1994), https://search.ieice.org/bin/summary.php?id=e77-d_12_1321.

[38] Ellysse Dick, *Balancing User Privacy and Innovation in Augmented and Virtual Reality*, **Info. Tech. & Innov. Found.** (Mar. 4, 2021), https://itif.org/publications/2021/03/04/balancing-user-privacy-and-innovation-augmented-and-virtual-reality/.

[39] Kurt Opsahl, *Come Back with a Warrant for my Virtual House*, **Elec. Frontier Found**. (Oct. 5, 2020), https://www.eff.org/deeplinks/2020/10/come-back-warrant-my-virtual-house.

[40] Morteza Dianatfar, Jyrki Latokartano, and Minna Lanz, *Review on existing VR/AR solutions in human–robot collaboration*, 97 **Procedia CIRP** 407 (2021), *accessible at* https://www.sciencedirect.com/science/article/pii/S2212827120314815; Courtney Bacon, *IVAS Mounted Amplifies Capabilities*, **U.S. Army Program Exec. Office Soldier** (Feb. 18, 2021), https://www.peosoldier.army.mil/News/Article-Display/Article/2508626/ivas-mounted-amplifies-capabilities/; Sanika Doolani, *A Review of Extended Reality (XR) Technologies for Manufacturing Training*, 8 **Technologies** 77 (2020), https://www.mdpi.com/2227-7080/8/4/77.

[41] Yehong Zhu, *How Niantic Is Profiting Off Tracking Where You Go While Playing 'Pokémon GO'*, **Forbes** (July 29, 2016), https://www.forbes.com/sites/yehongzhu/2016/07/29/how-niantic-is-profiting-off-tracking-where-you-go-while-playing-pokemon-go/?sh=3456e36b6df9.

[42] Open Letter from Daniel Leufer, Gaspar Pisanu, Estelle Masse, and Isedua Oribhabor on Nintendo's commitment to privacy on AR developments (Oct. 16, 2020) in **accessnow**, accessible at https://www.accessnow.org/cms/assets/uploads/2020/10/Access-Now-Letter-to-Nintendo.pdf; Nintendo of America, *Mario Kart Live: Home Circuit - Overview Trailer - Nintendo Switch*, **YouTube** (Oct. 1, 2020), https://www.youtube.com/watch?v=X6o6T40w6As.

[43] Jake Holland, *Meta's Facial Recognition Lawsuit Underscores Enforcement Risk*, **Bloomberg L.** (Feb. 15, 2022), https://news.bloomberglaw.com/privacy-and-data-security/metas-texas-facial-recognition-suit-shows-enforcement-headache.

[44] Josh Chin, *Chinese Police Add Facial-Recognition Glasses to Surveillance Arsenal*, **Wall St. J.** (Feb. 7, 2018), https://www.wsj.com/articles/chinese-police-go-robocop-with-facial-recognition-glasses-1518004353?mod=rss_Technology.

[45] Peter Casey, Ibrahim Baggili, and Ananya Yarramreddy, *Immersive Virtual Reality attacks and the Human Joystick*, 18 **IEEE Transactions on Dependable and Secure Computing** 550 (2019), *accessible at* https://www.researchgate.net/publication/332050743_Immersive_Virtual_Reality_Attacks_and_the_Human_Joystick.

[46] Thomas Alsop, *XR: AR, VR, and the metaverse - statistics & facts*, **Statista** (Oct. 20, 2022), https://www.statista.com/topics/6072/extended-reality-xr/.

[47] *Id*.

[48] Tim Pohlmann, *Rise in extended reality technology patents suggests market revival*, **IAM** (May 27, 2020), https://www.iam-media.com/article/rise-in-extended-reality-technology-patents-suggests-market-revival.

[49] Luiza Kirasirova, Vladimir Bulanov, Alexei Ossadtchi, Alexander Kolsanov, Vasily Pyatin, and Mikhail Lebedev, *A P300 Brain-Computer Interface With a Reduced Visual Field*, **Frontiers** (Dec. 3, 2020), https://www.frontiersin.org/articles/10.3389/fnins.2020.604629/full; Abdelkader Nasreddine Belkacem, Nuraini Jamil, Jason A. Palmer, Sofia Ouhbi and Chao Chen, *Brain Computer Interfaces for Improving the Quality of Life of Older Adults and Elderly Patients*, **Frontiers** (June 30, 2020), https://www.frontiersin.org/articles/10.3389/fnins.2020.00692/full.

[50] Joseph Makin, David Moses, and Edward Chang, *Machine translation of cortical activity to text with an encoder–decoder framework*, 23 **Nature Neuroscience** 575 (2020), *accessible at* https://www.nature.com/articles/s41593-020-0608-8.

[51] *Imagining a new interface: Hands-free communication without saying a word*, **Tech at Meta** (Mar. 30, 2020), https://tech.fb.com/ar-vr/2020/03/imagining-a-new-interface-hands-free-communication-without-saying-a-word/.

[52] Lynne Hall, Samiullah Paracha, Nicole Mitsche, Tom Flint, Fiona Stewart, Kate MacFarlane, Gill Hagan-Green, and Yvonne Dixon-Todd, *When Will Immersive Virtual Reality Have Its Day? Challenges to IVR Adoption in the Home as Exposed in Studies with Teenagers, Parents, and Experts*, **28 Presence: Virtual and Augmented Reality** 169 (2022), *accessible at* https://direct.mit.edu/pvar/article-abstract/doi/10.1162/pres_a_00347/108230/When-Will-Immersive-Virtual-Reality-Have-Its-Day?redirectedFrom=fulltext.

[53] Christopher Gorman, Recent Developments in AI and National Security: What You Need to Know, **Lawfare** (Mar. 3, 2022), https://www.lawfareblog.com/recent-developments-ai-and-national-security-what-you-need-know.

[54] Steve Blank, *Artificial Intelligence/Machine Learning and the Future of National Security*, **Small Wars J.** (May 11, 2022), https://smallwarsjournal.com/jrnl/art/artificial-intelligencemachine-learning-and-future-national-security.

[55] *Id*.

[56] Andrew Lohn, *Hacking Poses Risks for Artificial Intelligence*, **AFCEA Signal Mag.** (Mar. 1, 2022), https://www.afcea.org/content/hacking-poses-risks-artificial-intelligence.

[57] *Id*.

[58] *See generally* Srini Penchikala, *Analyzing and Preventing Unconscious Bias in Machine Learning*, **InfoQ** (Aug. 14, 2018), https://www.infoq.com/articles/machine-learning-unconscious-bias/.

[59] For an explanation on how natural language impacts machine learning, *see* Aylin Caliskan, *Detecting and Mitigating Bias in Natural Language Processing*, **Brookings Inst.** (May 10, 2021), https://www.brookings.edu/research/detecting-and-mitigating-bias-in-natural-language-processing.

[60] Maya Wang, *China's Techno-Authoritarianism Has Gone Global*, **Foreign Affairs** (Apr. 8, 2021), https://www.foreignaffairs.com/articles/china/2021-04-08/chinas-techno-authoritarianism-has-gone-global.

[61] Kevin Roose, *A.I.-Generated Art Is Already Transforming Creative Work*, **N.Y. Times** (Oct. 21, 2022), https://www.nytimes.com/2022/10/21/technology/ai-generated-art-jobs-dall-e-2.html.

[62] *Id*.

[63] Kelly Sayler and Laurie Harris, *Deep Fakes and National Security*, **Cong. Res. Serv.** (updated June 3, 2022), https://crsreports.congress.gov/product/pdf/IF/IF11333; Ian Sample, *What are deepfakes–and how can you spot them?*, **The Guardian** (Jan. 13, 2020), https://www.theguardian.com/technology/2020/jan/13/what-are-deepfakes-and-how-can-you-spot-them.

[64] *Increasing Threats of Deepfake Identities*, **U.S. Dept. of Homeland Security** (last visited Oct. 24, 2022), https://www.dhs.gov/sites/default/files/publications/increasing_threats_of_deepfake_identities_0.pdf.

[65] *Id*.

[66] *Id*.

[67] David Rodeck and Benjamin Curry, *What is Blockchain?*, **Forbes** (Apr. 28, 2022), https://www.forbes.com/advisor/investing/cryptocurrency/what-is-blockchain/.

[68] *See generally* Andrew Lisa, *NFT vs. Crypto:What Is the Difference*, **Go BankingRates** (June 29, 2022), https://www.gobankingrates.com/investing/crypto/nft-vs-crypto-what-is-the-difference/.

[69] Anshu Siripurapu, *Cryptocurrencies, Digital Dollars, and the Future of Money*, **Council on Foreign Relations** (Sept. 24, 2021), https://www.cfr.org/backgrounder/cryptocurrencies-digital-dollars-and-future-money.

[70] Andrew Ackerman, *What is a Central Bank Digital Currency and Should the U.S. Issue it?*, **Wall St. J.** (May 26, 2022), https://www.wsj.com/articles/should-the-u-s-issue-a-digital-dollar-which-could-compete-with-crypto-assets-11646921329.

[71] Tristan Bove, *Crypto Scams are Social Media's Latest Crisis*, **Fortune** (Jan. 31, 2022), https://fortune.com/2022/01/31/crypto-investment-fraud-scams-social-media-crisis-federal-trade-commission/.

[72] Cathy Hackl, *What are DAOs And Why You Should Pay Attention*, **Forbes** (June 1, 2021), https://www.forbes.com/sites/cathyhackl/2021/06/01/what-are-daos-and-why-you-should-pay-attention/?sh=329ea93f7305.

[73] *Id*.

[74] Max Dilendorf and Kareem Tabba, Forming and Operating a Wyoming DAO LLC, **Dilendorf** (June 8, 2021), https://dilendorf.com/resources/forming-and-operating-a-wyoming-dao-llc.html.

[75] *Kiva launches Africa's first national decentralized ID system with Hyperledger Indy*, **Hyperledger** (Jan. 20, 2021), https://www.hyperledger.org/wp-content/uploads/2021/01/Hyperledger_CaseStudy_Kiva_Printable.pdf.

[76] Priit Martinson, Estonia – the Digital Republic Secured by Blockchain, PricewaterhouseCoopers (2019), https://www.pwc.com/gx/en/services/legal/tech/assets/estonia-the-digital-republic-secured-by-blockchain.pdf.

[77] **Committee on the Future of Voting: Accessible, Reliable, Verifiable Technology, Securing the Vote: Protecting American Democracy** (2018), *accessible at* https://www.nap.edu/catalog/25120.

[78] Aline Oyamada, *El Salvador Buys More Bitcoin Despite 57% Loss and Debt Woes*, **Bloomberg** (July 1, 2022), https://www.bloomberg.com/news/articles/2022-07-01/el-salvador-buys-more-bitcoin-despite-57-loss-and-a-debt-crisis.

[79] Andrew Ackerman, *What is a Central Bank Digital Currency and Should the U.S. Issue it?*, **Wall St. J.** (May 26, 2022), https://www.wsj.com/articles/should-the-u-s-issue-a-digital-dollar-which-could-compete-with-crypto-assets-11646921329.

[80] Anil K. Jain, Patrick Flynn, and Aruna A. Ross, **Handbook of Biometrics** (2008), *accessible at* https://link.springer.com/book/10.1007/978-0-387-71041-9.

[81] *How Biometric Data is Stored*, **IEVO** (Dec. 10, 2020), https://ievoreader.com/how-biometric-data-is-stored/#:~:text=On%2Ddevice%20storage%20can%20be,t%20have%20control%20over%20it.

[82] *Biometrics*, **Dept. of Homeland Security** (last updated Dec. 14, 2021), https://www.dhs.gov/biometrics.

[83] Paul Bleicher, *Biometrics Comes of Age*, **Applied Clinical Trials** (Dec. 1, 2005), https://www.appliedclinicaltrialsonline.com/view/biometrics-comes-age.

[84] Blake Hannaford and Allison Okamura, *Haptics*, *in* **Springer Handbooks of Robotics** 1063-1084 (Bruno Siciliano and Oussama Khatib eds., 2016), *accessible at* https://link.springer.com/chapter/10.1007/978-3-319-32552-1_42.

[85] *Id*.

[86] Peter Shull and Dana Damian, *Haptic wearables as sensory replacement, sensory augmentation and trainer – a review*, 12 **J. of NeuroEngineering and Rehabilitation** 59 (2015), *accessible at* https://link.springer.com/article/10.1186/s12984-015-0055-z.

[87] Aashish Mehra, *Haptic Technology Market worth $4.6 billion* by 2026, **MarketsandMarkets** (Jan. 22, 2021), https://www.marketsandmarkets.com/PressReleases/haptic-technology.asp.

[88] Grzegorz Zwoliński, Dorota Kamińska, Anna Laska-Leśniewicz, and Łukasz Adamek, *Vibrating Tilt Platform Enhancing Immersive Experience in VR*, 11 **Electronics** 462 (2022), *accessible at* https://www.mdpi.com/2079-9292/11/3/462/htm.

[89] Shujie Deng and Jian Chang, *A Survey of Haptics in Serious Gaming*, **Second Intl. Conf., Games and Learning Alliance** (2013), https://www.researchgate.net/publication/279924358_A_Survey_of_Haptics_in_Serious_Gaming.

[90] Anna Morgan-Thomasa, Laurence Dessartb, and Cleopatra Veloutsou, *Digital ecosystem and consumer engagement: A socio-technical perspective*, 121 **J. of Bus. Res.** 713 (2020), accessible at https://www.sciencedirect.com/science/article/pii/S0148296320302150?casa_token=JBKRuTdDOWUAAAAA:bKHifSiJB_Jh1sw5vt8AwKUOyEopWJdH4EiedLIDsYytYP_42RE4Y38Acy-RKOjw4AbRWQLQfISP.

[91] Pedro Palandrani, *The Metaverse Takes Shape as Several Themes Converge*, **Global X** (Sept. 13, 2021), https://globalxetfs.co.jp/en/research/the-metaverse-takes-shape-as-several-themes-converge/index.html.

[92] William G. Gilroy, *Questions raised about iris recognition systems*, **ScienceDaily** (July 12, 2012), https://www.sciencedaily.com/releases/2012/07/120712141938.htm.

[93] Soyuj Kumar Sahoo, Tarun Choubisa, and Mahadeva Prasanna, *Multimodal Biometric Person Authentication : A Review*, 29 **IETE Technical Rev.** 54 (2012), *accessible at* https://web.archive.org/web/20140116103048/http://tr.ietejournals.org/text.asp?2012%2525252f29%2525252f1%2525252f54%2525252f93139.

[94] *See generally* Jessica Groopman, *In Biometrics, Security Concerns Span Technical, Legal, and Ethical*, **TechTarget** (June 2020), https://www.techtarget.com/searchsecurity/tip/In-biometrics-security-concerns-span-technical-legal-and-ethical.

[95] Zao Feng, Xi Zhao, Bogdan Carbunar, and Weidong Shi, *Continuous Mobile Authentication Using Virtual Key Typing Biometrics*, **IEEE Intl. Conf. on Trust, Security and Privacy in Computing and Communications** (2013), *accessible at* https://ieeexplore.ieee.org/abstract/document/6681014?casa_token=p3Q7XTh7swMAAAAA:FpXkY4sLx4Ed75d3WUxUhNRIZ9sk-_kC-l9qyIiHY3AegVLf8enbUtUhCABuNVhGSRYHI0vH1Fo.

[96] M. Orozco, Y. Asfaw, S. Shirmohammadi, A. Adler, and A. el Saddik, *Haptic-Based Biometrics: A Feasibility Study*, **IEEE Symp. on Haptic Interfaces for Virtual Env. and Teleoperator Sys.** (2006), *accessible at* https://ieeexplore.ieee.org/abstract/document/1627094.

[97] Charles Duhigg, *How Companies Learn Your Secrets*, **N.Y. Times** (Feb. 19, 2012), https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html.

[98] Carly Page, *Supreme Court overturns Roe v. Wade: Should you delete your period-tracking app*?, **TechCrunch** (May 5, 2022), https://techcrunch.com/2022/05/05/roe-wade-privacy-period-tracking/.

[99] *See generally* Rotimi Onadipe, *The Importance of Cyber Awareness in Today's Digital Age*, **The Cable** (Apr. 23, 2021), https://www.thecable.ng/the-importance-of-cyber-security-awareness-in-todays-digital-age; Kurt Baker, *What Is Cyber Espionage?*, **Crowdstrike** (June 1, 2022), https://www.crowdstrike.com/cybersecurity-101/cyberattacks/cyber-espionage/.

[100] *What We Investigate*, **FBI** (last visited Oct. 24, 2022), https://www.fbi.gov/investigate/cyber.

[101] William Largent, *New VPNFilter malware targets at least 500K networking devices worldwide*, **Talos Intelligence** (May 23, 2018), https://blog.talosintelligence.com/2018/05/VPNFilter.html.

[102] John Hoehn and Kelley Sayler, *National Security Implications of Fifth Generation (5G) Mobile Technologies*, **Cong. Res. Serv.** (updated Apr. 5, 2022), https://sgp.fas.org/crs/natsec/IF11251.pdf.

[103] *Id*.

[104] Jason S. Boswell, *5G network security is national security*, **Ericsson** (Apr. 23, 2020), https://www.ericsson.com/en/blog/2020/4/5g-network-security-is-national-security.

[105] Sam Smith, *CYBERSECURITY BREACHES TO RESULT IN OVER 146 BILLION RECORDS BEING STOLEN BY 2023*, **Juniper Research** (updated Aug. 2022), https://www.juniperresearch.com/press/cybersecurity-breaches-to-result-in-over-146-bn.

[106] Jason S. Boswell, *5G network security is national security*, **Ericsson** (Apr. 23, 2020), https://www.ericsson.com/en/blog/2020/4/5g-network-security-is-national-security.

[107] Andrew Eversden, *National security agencies warn of 5G network vulnerabilities, adversary influence*, **c4isernet** (May 10, 2021), https://www.c4isrnet.com/battlefield-tech/it-networks/5g/2021/05/10/national-security-agencies-warn-of-5g-network-vulnerabilities-adversary-influence/.

[108] Michael A. Solitro, *Rural Communities Launch Publicly Owned Fiber Networks*, **Broadband Communities Magazine** (2021), https://www.bbcmag.com/community-broadband/rural-communities-launch-publicly-owned-fiber-networks.

[109] Anna Read and Lily Gong, *States Considering Range of Options to Bring Broadband to Rural America*, **Pew** (Mar. 29, 2022), https://www.pewtrusts.org/en/research-and-analysis/articles/2022/03/29/states-considering-range-of-options-to-bring-broadband-to-rural-america.

[110] Press Release, Federal Communications Commission, FCC Announces Over $1 Billion in Rural Broadband Support to 32 States (Dec. 16, 2021), https://www.fcc.gov/document/fcc-announces-over-1-billion-rural-broadband-support-32-states.

[111] Press Release, White House, FACT SHEET: Biden-Harris Administration Mobilizes Resources to Connect Tribal Nations to Reliable, High-Speed Internet (Dec. 22, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/12/22/fact-sheet-biden-harris-administration-mobilizes-resources-to-connect-tribal-nations-to-reliable-high-speed-internet/.

[112] Eduardo Porter, *A Rural-Urban Broadband Divide, but Not the One You Think Of*, **N.Y. Times** (June 1, 2021), https://www.nytimes.com/2021/06/01/business/rural-urban-broadband-biden.html.

[113] *Id*.

[114] Adam Clark Estes, *How the Technology Behind Airplane Wifi Could Help Connect Everyone on Earth*, Vox (Sept. 26, 2020), https://www.vox.com/recode/2020/9/26/21457530/elon-musk-spacex-starlink-satellite-broadband-amazon-project-kuiper-viasat.

[115] Julia Siegal, *Commercial satellites are on the front lines of war today. Here's what this means for the future of warfare*, **Atlantic Council** (Aug. 30, 2022), https://www.atlanticcouncil.org/content-series/airpower-after-ukraine/commercial-satellites-are-on-the-front-lines-of-war-today-heres-what-this-means-for-the-future-of-warfare/.

[116] Christian Zilles, *Why Space Is the Final Frontier for Social Media*, **Social Media HQ** (Dec. 18, 2020), https://socialmediahq.com/why-space-is-the-final-frontier-for-social-media/.

[117] Jon Porter, *Facebook's satellite internet team joins Amazon*, **The Verge** (July 14, 2021), https://www.theverge.com/2021/7/14/22576788/amazon-acquires-facebook-satellite-team-project-kuiper.

[118] Tim Starks, *Cyberattacks on satellites may only be getting more worrisome*, **Wash. Post** (July 29, 2022), https://www.washingtonpost.com/politics/2022/07/29/cyberattacks-satellites-may-only-be-getting-more-worrisome/.

[119] *Id*.

[120] Michael Tabb, Andrea Gawrylewski, and Jeffery DelViscio, *How Does a Quantum Computer Work*, **Scientific American** (July 7, 2021), https://www.scientificamerican.com/video/how-does-a-quantum-computer-work/.

[121] *Id*.

[122] Liam Tung, *Amazon and Microsoft want to go big on data centres, but the power grid can't support them*, **ZD NET** (Aug. 23, 2022), https://www.zdnet.com/article/power-shortages-threat-aws-and-microsofts-eu-data-center-expansion/.

[123] Tim De Chant, *Biden's new restrictions on exporting semiconductor tools hit China where it hurts*, **TechCrunch** (Oct. 18, 2022), https://techcrunch.com/2022/10/18/bidens-new-restrictions-on-exporting-semiconductor-tools-hit-china-where-it-hurts/.

[124] *Id*.

[125] *See, e.g.*, **The Mighty** (last visited Oct. 24, 2022), https://themighty.com/.

[126] *See, e.g., Vanderbilt University and Dysautonomia International Launch "The Big POTS Survey" To Study the Impact of Postural Tachycardia Syndrome*, **Dysautonomia Intl.** (last visited Oct. 24, 2022), https://www.dysautonomiainternational.org/page.php?ID=48.

[127] *Current Time*, **Bulletin of the Atomic Scientists** (updated Jan. 20, 2022), https://thebulletin.org/doomsday-clock/current-time/.

[128] *See generally* Rianna Walcott, *WhatsApp aunties and the spread of fake news*, **Wellcome Collection** (July 7, 2020), https://wellcomecollection.org/articles/Xv3T1xQAAADN3N3r; Lili Pike, *How china uses global media to spread its views – and misinformation*, **GRID** (May 18, 2022), https://www.grid.news/story/global/2022/05/18/how-china-uses-global-media-to-spread-its-views-and-misinformation/.

[129] Zeyi Yang, *Now China wants to censor online comments*, **MIT Tech. Rev.** (June 18, 2022), https://www.technologyreview.com/2022/06/18/1054452/china-censors-social-media-comments/.

[130] *The Social Dilemma: Social Media and Your Mental Health*, **McLean Hospital** (Jan. 21, 2022), https://www.mcleanhospital.org/essential/it-or-not-social-medias-affecting-your-mental-health.

[131] Anne Speckhard, *How Do Those Vulnerable to Terror Recruitment Respond to YouTube Counter-Narrative Videos*?, **Homeland Security Today** (Mar. 30, 2021), https://www.hstoday.us/subject-matter-areas/counterterrorism/how-do-those-vulnerable-to-terror-recruitment-respond-to-youtube-counter-narrative-videos/.

[132] *See generally* Jessica Souza, *3 Ways to Spot a Trafficker on Social Media*, **Plan Intl.** (Jan. 5, 2022), https://www.planusa.org/blog/3-ways-to-spot-a-trafficker-on-social-media/; *See also* Clarence Williams, *FBI warns of online sextortion schemes targeting teens*, **Wash. Post** (Mar. 24, 2022), https://www.washingtonpost.com/dc-md-va/2022/03/24/fbi-warns-online-sextortion-scams-target-teens/.

[133] Louis Lucero and Melissa Gomez, *Richard Russell Stole a Plane in Seattle and Crashed It. How'd He Learn to Fly?*, **N.Y. Times** (Aug. 12, 2018), https://www.nytimes.com/2018/08/12/us/richard-russell-q400-flight-simulator.html.

[134] Elizabeth Chuck, *Witness intimidation on social media: law enforcement's growing challenge*, **NBC News** (Nov. 15, 2013), https://www.nbcnews.com/news/us-news/witness-intimidation-social-media-law-enforcements-growing-challenge-flna2d11599928.

[135] *See generally* Laura K. Donohue, *The Limits of National Security*, 48 **Am. Crim. L. Rev.** 1573 (2011), https://scholarship.law.georgetown.edu/facpub/1010/.

[136] John Thornhill, *Democracies must use AI to defend open societies*, **Financial Times** (Aug. 25, 2022), https://www.ft.com/content/a4e8da53-84e2-498b-82f6-1b01e1291bd9.

[137] For example, the Federation of American Scientists and others have explored the idea. Saiph Savage, Cristina Martinez Pinto, Shannon Biega, Claudia Flores-Saviaga, and Luz Elena Gonzalez, *A National Cloud for Conducting Disinformation Research at Scale*, **Day One Proj.** (June 29, 2021), https://www.dayoneproject.org/ideas/a-national-cloud-for-conducting-disinformation-research-at-scale.

[138] For an example of Uber's business model, *see* David Trainer, *the Emperor Has No Clothes – Uber's Business Model is Broken*, **Forbes** (Sept. 9, 2020), https://www.forbes.com/sites/greatspeculations/2020/09/09/the-emperor-has-no-clothes--ubers-business-model-is-broken/?sh=5cd26c13706a. For an example of regulatory shortcomings of Uber, *see also* Gad Allon and John Paul MacDuffie, *Can Uber Overcome Its Regulatory Obstacles?*, **Knowledge at Wharton** (Dec. 3, 2019), https://knowledge.wharton.upenn.edu/article/can-uber-overcome-regulatory-obstacles/.

[139] *See generally Risks and challenges of data access and sharing, in* **Enhancing Access to and Sharing of Data** (OECD eds., 2019), accessible at https://www.oecd-ilibrary.org/sites/15c62f9c-en/index.html?itemId=/content/component/15c62f9c-en.

[140] Max Freedman, *How Businesses Are Collecting Data (And What They're Doing With It)*, **Bus. News Daily** (Aug. 25, 2022), https://www.businessnewsdaily.com/10625-businesses-collecting-data.html.

[141] *Id.*

[142] Michael Levenson and April Rubin, *Parents Sue TikTok Saying Children Died After Viewing Blackout Challenge*, **N.Y. Times** (July 6, 2022), https://www.nytimes.com/2022/07/06/technology/tiktok-blackout-challenge-deaths.html.

[143] Jeff Bercovici, *Sorry, Craig: Study Finds Craigslist Took $5 Billion From Newspapers*, **Forbes** (Aug. 14, 2013), https://www.forbes.com/sites/jeffbercovici/2013/08/14/sorry-craig-study-finds-craigslist-cost-newspapers-5-billion/?sh=26e84da17d02.

[144] *Transforming Lives*, **USAID** (updated July 12, 2021), https://www.usaid.gov/results-data/success-stories/young-journalists-start-faktoje-albania%25E2%2580%2599s-first-fact-checking-news.

[145] *See, e.g.*, Nicola Jones, *How to stop data centres from gobbling up the world's electricity*, **nature** (Sept. 12, 2018), https://www.nature.com/articles/d41586-018-06610-y.

[146] Chloe Taylor, *Silicon Valley giants accused of avoiding over $100 billion in taxes over the last decade*, **CNBC** (Dec. 2, 2019), https://www.cnbc.com/2019/12/02/silicon-valley-giants-accused-of-avoiding-100-billion-in-taxes.html.

[147] *See generally* Ricardo Baeza-Yates, *Bias on the Web*, 61 **Commun. of the ACM** 54 (2018), accessible at https://cacm.acm.org/magazines/2018/6/228035-bias-on-the-web/fulltext.

[148] *See* **Nir Eyal, Hooked** (2014), *accessible at* https://www.nirandfar.com/hooked/.

[149] *See e.g.*, Sean Illing, *"Flood the zone with shit": How misinformation overwhelmed our democracy*, **Vox** (Feb. 6, 2020), https://www.vox.com/policy-and-politics/2020/1/16/20991816/impeachment-trial-trump-bannon-misinformation.

[150] For an explanation of filter bubbles and confirmation bias, *see Filter bubbles & confirmation bias*, **Reynolds Comm. College Libraries** (updated Oct. 23, 2022), https://libguides.reynolds.edu/fakenews/bias.

[151] Quarterly Letter to LPs, Lux Capital (2022), https://drive.google.com/file/d/1yCXj_kRbfvZvehTCrZRrPPwN7Vn2rMEx/view.

[152] *About CISA*, **Cybersecurity & Infrastructure Security Agency** (last visited Oct. 24, 2022), https://www.cisa.gov/about-cisa.

[153] *Mis, Dis, Malinformation*, **Cybersecurity & Infrastructure Security Agency** (updated Oct. 18, 2022), https://www.cisa.gov/mdm.

[154] *Id.*

[155] *Homeland Security Investigations*, **U.S. Immigration and Customs Enforcement** (updated Aug. 16, 2022), https://www.ice.gov/about-ice/homeland-security-investigations.

[156] *U.S. Secret Service (USSS)*, **Dept. of Homeland Security** (updated Dec. 16, 2021), https://www.dhs.gov/employee-resources/us-secret-service-usss.

[157] *Cyber Safety Review Board*, **Cybersecurity & Infrastructure Security Agency** (last visited Oct. 24, 2022), https://www.cisa.gov/cyber-safety-review-board.

[158] *Global Engagement Center*, **U.S. Dept. of State** (updated Oct. 11, 2022), https://www.state.gov/bureaus-offices/under-secretary-for-public-diplomacy-and-public-affairs/global-engagement-center/.

[159] *Technology Engagement Team*, **U.S. Dept. of State** (last visited Oct. 24, 2022), https://www.state.gov/bureaus-offices/under-secretary-for-public-diplomacy-and-public-affairs/global-engagement-center/technology-engagement-team.

[160] Maggie Miller, *Blinken formally announces new State Department cyber bureau*, **The Hill** (Oct. 27, 2021), https://thehill.com/policy/cybersecurity/578728-blinken-formally-announces-new-state-dept-cyber-bureau-as-part-of/.

[161] *Id. See also* Cyber Diplomacy Act of 2021, H.R. 1251, 117th Cong. (2021) (passed House on April 20th, 2021).

[162] Media Note, Office of the Spokesperson, *Establishment of the Bureau of cyberspace and Digital Policy*, **U.S. Dept. of State** (Apr. 4, 2022), https://www.state.gov/establishment-of-the-bureau-of-cyberspace-and-digital-policy/.

[163] *Members of the IC*, **Office of the Dir. of Natl. Intel.** (last visited on Oct. 24, 2022), https://www.dni.gov/index.php/what-we-do/members-of-the-ic.

[164] *Our Mission and Vision*, **U.S. Cyber Command** (last visited Oct. 24, 2022), https://www.cybercom.mil/About/Mission-and-Vision/.

[165] **National Security Agency/Central Security Service** (last visited Oct. 24, 2022), https://www.nsa.gov/.

[166] FY2022 - 2026 ODNI S&T Investment Landscape, Office of the Director of National Intelligence (Feb. 28, 2022), https://sam.gov/opp/15d5927d5c5345939830e882856d2fca/view.

[167] Lauren Williams, *The IC's 4-year emerging tech investment plan*, **FCW** (Mar. 18, 2022), https://fcw.com/acquisition/2022/03/ics-4-year-emerging-tech-investment-plan/363348/.

[168] *Id*.

[169] *How We Work*, **In-Q-Tel** (updated 2022), https://www.iqt.org/how-we-work/.

[170] *In-Q-Tel Engagement*, **Dept. of Homeland Security** (updated Apr. 11, 2022), https://www.dhs.gov/science-and-technology/iqt.

[171] *How We Work*, **In-Q-Tel** (updated 2022), https://www.iqt.org/how-we-work/.

[172] *In-Q-Tel Engagement*, **Dept. of Homeland Security** (updated Apr. 11, 2022), https://www.dhs.gov/science-and-technology/iqt.

[173] Statement of FBI Director Christopher Wray Before the Senate Appropriations Committee, Subcommittee on Commerce, Justice, Science, and Related Agencies (May 25, 2022) (discussing the FBI's cyber efforts in past and upcoming fiscal years), https://www.fbi.gov/news/testimony/federal-bureau-of-investigation-budget-request-for-fiscal-year-2023.

[174] *What the FTC Does*, **Fed. Trade. Commission** (last visited on Oct. 24, 2022), https://www.ftc.gov/news-events/media-resources/what-ftc-does.

[175] *See, e.g., Case Summary, FTC v. Facebook, Inc.*, **Fed. Trade Commission** (updated Nov. 17, 2021), https://www.ftc.gov/legal-library/browse/cases-proceedings/191-0134-facebook-inc-ftc-v.

[176] Memorandum from Chairwoman Lina M. Khan to Commission Staff and Commissioners, Federal Trade Commission (Sept. 22, 2021), https://www.ftc.gov/system/files/documents/public_statements/1596664/agency_priorities_memo_from_chair_lina_m_khan_9-22-21.pdf.

[177] *The Importance of Artificial Intelligence and Data for the Telecommunications Industry and the FCC*, **Fed. Communications Commission** (Jan. 14, 2021), https://www.fcc.gov/sites/default/files/fcc_aiwg_2020_whitepaper_final.pdf.

[178] *About the SEC*, **U.S. Securities and Exchange Commission** (updated Nov. 22, 2016), https://www.sec.gov/about.shtml.

[179] **Commodity Futures Trading Commission** (last visited Oct. 24, 2022), https://www.cftc.gov/.

[180] *Strategic Plan 2020-2024*, **Commodity Futures Trading Commission** (July 8, 2020), https://www.cftc.gov/media/3871/CFTC202024_2024StrategicPlan/download.

[181] Report, The CFTC's Role in Monitoring Virtual Currencies, Commodity Futures Trading Commission (2020), https://www.cftc.gov/media/4636/VirtualCurrencyMonitoringReportFY2020/download.

[182] Joseph Evans and Alexandra Scheibe, *A Flurry of CFTC Actions Shock the Cryptocurrency Industry*, **The Natl. L. Rev.** (Oct. 1, 2022), https://www.natlawreview.com/article/flurry-cftc-actions-shock-cryptocurrency-industry.

[183] Abe Chernin, Nicole M. Moran, and Simona Mola, *The CFTC's Approach to Virtual Currencies*, **The Natl. L. Rev.** (Dec. 21, 2020), https://www.natlawreview.com/article/cftc-s-approach-to-virtual-currencies.

[184] 12 U.S.C. §§ 5562–65.

[185] Hunton Andrews Kurth, *CFPB Orders Six Tech Companies to Provide Information on Payment Systems Data Practices*, **The Natl. L. Rev.** (Nov. 4, 2021), https://www.natlawreview.com/article/cfpb-orders-six-tech-companies-to-provide-information-payment-systems-data-practices.

[186] Kristin Finklea, *Law Enforcement and Technology: Using Social Media*, **Cong. Res. Serv.** (Jan. 11, 2022), https://crsreports.congress.gov/product/pdf/R/R47008.

[187] The Cipher Brief, *The CIG's Innovation Debate: How 1929 & the Formation of the SEC Can Help | The Cipher Brief*, **YouTube** (Apr. 13, 2022), https://www.youtube.com/watch?v=fi1YvLAIRu0.

[188] *Id*.

[189] Comments of the Direct Market Association Before the U.S. Dept. of Commerce (July 6, 1998), *accessible at* https://www.ntia.doc.gov/legacy/ntiahome/privacy/mail/disk/DMA.htm.

[190] Ethan Zuckerman, *The Case for Digital Public Infrastructure*, **Knight First Amend. Inst. at Columbia Univ.** (Jan. 17, 2020), https://knightcolumbia.org/content/the-case-for-digital-public-infrastructure.

[191] *Id*.

[192] *Id*.

[193] *Id*.

[194] Andrew Selsky, *Oregon might dump controversial spyware investment*, **Assoc. Press** (Dec. 17, 2021), https://apnews.com/article/technology-business-oregon-spyware-berkeley-7ed2f216d4d462998080d166cc823aae.

[195] As enforced by government actors, this right may run into First Amendment concerns if applied too liberally to activities like "spoofing" an email where the activity is not criminal. Private sector actors would have far more latitude to implement this right, and satire would be protected in any case.

[196] An individual's sale of their data is covered by a right to contract, and thus could compromise some protections under this right, depending on the agreed upon terms.

[197] Note that this right may raise First Amendment concerns, but our Task Force experts were not convinced that such concerns were constitutionally sound or insurmountable for effective implementation.

[198] The threshold for a "major" decision must be quite high. As platforms take over more of the public square and assume major societal functions, the concept of integrating democratic decision making into platforms must be at least explored to preserve the democratic nature of American governance.

[199] For additional ideas, *see* Edmund L. Andrews, *Rob Reich: AI Developers Need a Code of Responsible Conduct*, **HAI** (June 22, 2022), https://hai.stanford.edu/news/rob-reich-ai-developers-need-code-responsible-conduct.

[200] Examples of some potential metric areas from 7 Pillars Global Insights, oriented at company evaluations, include: Does the company host or support programs aimed at enhancing the ability of employees, particularly in digital spaces, to recognize hate speech, targeted disinformation and conspiracy theories? Does the company encourage and support independent local journalism? Does the company fund external civic education programs aimed at combatting disinformation? Does the company donate to politicians that have a track record of spreading disinformation? Does the company have a policy on advertising on networks or programs that perpetuate disinformation about the 2020 election or upcoming elections, that otherwise promote baseless claims about election fraud, or that incite attacks targeting state election officials? Does the company publicly endorse government efforts to address disinformation? Mark S, Bergman, *The Next Frontier in ESG: Speaking Out in Support of Democracy*, **7Pillars Global Insights** (Apr. 4, 2022), https://www.7pillarsglobal-insights.com/_files/ugd/24200f_4d90e4734a2346cdbd5de97b72162411.pdf.

[201] John Thornhill, *Democracies must use AI to defend open societies*, **Financial Times** (Aug. 25, 2022), https://www.ft.com/content/a4e8da53-84e2-498b-82f6-1b01e1291bd9.

[202] The scenario construction owes a debt of gratitude to the National Security Crisis Law Simulation Core Control Team members who for more than a decade helped to build the simulations run by Professor Laura K. Donohue. Applied to the social media universe, the scenarios developed represent the next logical step in understanding future threats to US national security.

600 New Jersey Ave., NW | Gewirz 308 | Washington D.C., 20001
(202) 662–4072 | email: nationalsecurity@law.georgetown.edu
www.law.georgetown.edu/national-security-center