EVENT BRIEFING

Digital Technologies

Frontier technologies offer many exciting commercial opportunities to investors as they promise to fundamentally transform manufacturing and logistics, as well as open new markets around the world. Applications of frontier technologies, in particular artificial intelligence and biotechnologies, also offer unprecedented opportunities to advance health care and development in communities and nations of the emerging world.

To realize the upsides and promises of new technologies, investors must also have a strong understanding to the potential risks these technologies pose. Current assessments of opportunities and risks in ventures primarily focus on three elements:

- *Product* looks at the technical viability and user-friendliness of the product itself.
- *Market* looks at the overall market size, market growth rates, and an assessment of the competition.
- *Team* looks at the professional background and personality profiles of the founders and assesses the degree to which they will be able to execute on their plan.

Although often overlooked, a fourth dimension, *Societal Impacts*—and in particular, how key stakeholders such as customers, communities, and governments will respond to a disruptive business model or new technology - is also critical to achieving commercial success, and should be just as central to investment process.

Mature Digital Technologies: What to Consider

Digital technologies cover a broad spectrum from IT services, telecoms, software systems, and digital platform services. The Sustainability Accounting Standards Board (SASB), an entity which sets standards for ESG disclosure and evaluation by investors, has identified material issues which should be closely evaluated:[1]

- Environmental Footprint of Hardware Infrastructure
- Data Privacy & Freedom of Expression
- Data Security
- Recruiting & Managing a Global, Diverse Skilled Workforce
- Managing Systemic Risks from Technology Disruptions
- Intellectual Property Protection & Competitive Behavior

The standards encompass a broad range of issues including advancing skills upgrading and diversity in the technology workforce, managing the regulatory environment for immigration, protecting intellectual property and fair competition, and managing the environmental footprint of hardware and operations. Two areas which have received a high level of recent scrutiny for telecoms and software companies are Data Privacy and Security and Freedom of Expression.

Data Privacy and Security

Data privacy involves the full life cycle of collection, storage, sharing, and destruction of user data. Companies typically conduct a *Privacy Impact Assessment* that explains what information is collected, the intended use of the information, the ability of users to decline to collection or specific uses of data, and how the security of data is maintained. A rapidly changing landscape of public awareness[2] and regulatory actions on protecting privacy[3] could greatly impact the types of business models that will be feasible in the coming years.

Elements of Data Privacy

- *Notification* refers to whether users must be informed that their data is being collected and which types of data.
- *Consent* refers to whether a user must give permission for data to be collected and if the user has an opportunity to opt-out.
- *Correction and Deletion* refers to whether users have an opportunity to correct or to request deletion of their data.

- *Security* refers to the encryption and security processes used to store and share data. Certain types of data require additional protections.

Types of Data

- *Personal data* refers to data that is unique to identifying an individual such as name and email address. It may also refer to certain profiles of data that may lead to a unique identification such as geolocation tracking over time.
- *Sensitive data* is data that legally requires additional consideration for its treatment and use which can include data on an individual's education, health, and financial records.

Freedom of Expression

Freedom of expression involves the use of digital technologies for the communication and distribution of speech, graphics, and other forms of communication. With the rise of digital platforms such as Facebook, Twitter, Instagram, and other platforms over the last decade, a number of issues have surfaced. Most issues come down to specific platform design and management choices.

- *Anonymity* is a policy choice about if an individual may use a platform without disclosing (and verifying) their identity to either the platform operator or to other users on the platform. Higher allowances on anonymity can lead to increases in fraud and misinformation. During major news events, it is estimated that 40-60% of Twitter traffic is activity by Bots.[4]
- *Community standards* involve the terms and conditions under which one may use a platform and the types of content that may be shared.
- *Content blocking* is the degree to which a company is actively monitoring a platform and removing content. This can be done for legal purposes such as copyright infringement or preventing child pornography dissemination. It may also be done to maintain community standards around hate speech, cyberbullying, indecency, and personal attacks, or to suppress speech not in line with values, beliefs, or commercial interests of the platform owner. Governments also engage in content blocking, typically by blocking URLs to websites that are determined to infringe on or undermine national cultural values or other societal concerns.
- *Content curation* is the practice of verifying accuracy and quality of information on a digital media platform. '*Disinformation*' is a related concern that refers to how companies manage platform users who are operating targeted campaigns to spread false or misleading information for ideological, commercial, or political purposes.
- *Network disruptions* involve state-mandated temporary shutdowns of internet service providers, cellular networks, or blocking of social media sites. In 2018 there were 188 incidents of internet shutdowns worldwide, most having to do with political protests and campaigns.[5] The costs to companies engaged in network disruptions can be immense –both from broken trust with customers and in subsequent legal actions.[6]

Governance of Digital Technologies

The current governance approach to managing digital rights, privacy, and freedom of expression matters centers on establishing voluntary principles and improving transparency of company practices. The *Global Network Initiative (GNI),* founded in 2008, established the GNI Principles[7], a set of commitments by companies to reduce government interference in free expression and violations of individual privacy. Current signatories to the GNI Principles include Microsoft, Google, Telenor, Vodafone, and Orange, among others. GNI conducts confidential company assessments and presents results in anonymized reports.

Transparency and Rankings

There are several new initiatives to advance transparency into the privacy and security practices of the largest tech companies.

- *JUST Capital*[8] provides ranking of more than 800 companies' performance on ESG issues including customer privacy.
- *Ranking Digital Rights (RDR) Index*[9] ranks the largest telecoms and digital platform companies on their performance on issues of corporate governance, cybersecurity, privacy, and freedom of expression.
- *Transparency Reporting Index*[10] by Access Now provides links to companies' voluntary self-reporting on government requests to share user data and censor content.

Frontier Digital Technologies: What to Consider

Frontier digital technologies have many of the same concerns as today's digital technologies, but they also have a range of additional concerns that investors should be tracking.

Artificial Intelligence

Artificial intelligence is a field of computer science that seeks to create software products that are capable of mimicking human cognition and decision-making processes. The field encompasses a broad range of techniques and applications.

Types of AI

- *Machine Learning* leverages large data sets to infer patterns and trends to render a prediction or decision on outcomes. Machine learning applications can be found in nearly every industry—ranging from targeted advertisements based on past browsing history, to medical diagnostics based on medical records and genetics, to sentencing and parole guidelines based on past recidivism rates.
- *Computer Vision* processes images and videos to identify patterns and trends. Applications include facial recognition software for social media apps and law enforcement, as well as detecting cancer in radiological scans.
- *Natural Language Processing* develops methods for computers to understand human speech. Applications include translators and Digital Assistants like Amazon Alexa and Siri.

Governance of AI

There has been widespread interest in understanding the ethics of AI. Over the last several years, more than two dozen organizations have publicly issued AI ethics principles. Among the most notable AI principles are the Asilomar Principles[11] and the IEEE Ethics in Action standards.[12] Some large tech companies[13] including Microsoft, Google, and IBM have also issued public statements on their own AI ethics principles. While each set of principles varies, they contain common themes.

- *Fairness* refers to whether algorithms represent commonly accepted norms of fairness in the context where the algorithms are applied, such as employment promotion decisions within a particular company or broader national societal norms .
- *Anti-discrimination* (also called 'bias') refers to whether the algorithm will prevent reinforcing pre-existing structural biases in decisions. This is particularly important where algorithms affect outcomes to historically marginalized groups such as the poor, women, minorities, and persons with disabilities.
- *Transparency* refers to whether the inputs and weighting of variables in the algorithm are shared with those impacted.
- *Accountability* refers to whether an individual or organization takes responsibility for the decisions informed by the algorithm. It can also refer to whether there is a process to appeal a decision rendered by an algorithm.
- *Privacy* refers to the protection of user data included in an algorithm.
- *Scientific integrity* refers to the data science standards used in collection and analysis of data for the algorithm.
- *Diversity* refers to the range of stakeholders who are involved in the design, testing, and oversight of the algorithm.
- *Safety* refers to anticipation and mitigation of harm that could result based on an algorithm. This is especially important in contexts where life and death decisions are made such as military, autonomous vehicles, and medical treatments.
- *Applications* refers to specific customers or activities that a company will or will not serve with AI products. For example, Google's AI Principles exclude specific applications: "Technologies that cause or are likely to cause overall harm…Weapons or other technologies whose principal purpose or implementation is to cause or directly facilitate injury to people. Technologies that gather or use information for surveillance violating internationally accepted norms..."[14]

Internet of Things

There are currently around 25 billion Internet of Things (IoT) devices worldwide—a number expected to rise to 75 billion by 2025. [15] Bain estimates that total spending on IoT in 2022 could reach $545 Billion.[16] IoT devices encompass a broad range of products including integrated sensors in manufacturing and supply chains; 'smart home' devices such as locks, thermostats, and controls for lighting and appliances; 'smart city' controls on traffic lights and

self-driving cars; medical devices and consumer health wearable devices such as smart watches; and sensor controlled devices like insulin pumps.

Cybersecurity

IoT is opening a new realm of vulnerability for companies, as cybersecurity attacks move from accessing data to manipulating physical objects such as door locks, traffic lights, and power grids. A survey by Bain found that cybersecurity concerns are the top barrier preventing adoption of IoT solutions among companies, followed by data interoperability and vendor risk.[17]

Medical devices with linked sensors have faced similar security challenges. These devices have been targeted for cyberattacks, and their manufacturers have faced increasing scrutiny for not having adequate protections against vulnerabilities.[18] Frontier neurotechnology devices currently in development, such as EEG headsets for drone and AV control and Brain-Computer Interfaces for 'hands-free keyboards', will create even more cybersecurity vulnerabilities. Lab tests conducted on EEG headsets have shown that subliminal messaging can be used in 'phishing attacks' to extract sensitive information such as banking PIN codes.[19]

5G Networks

IoT will be enabled by 5G mobile networks. The method in which 5G is deployed, as well as its oversight and governance, have the potential to help navigate the challenges of cybersecurity and interoperability.[20] Some observers have raised concerns that 5G connectivity will largely be concentrated in urban areas and higher income communities—further widening the existing broadband *digital divide* in U.S. communities and between advanced and emerging nations.[21]

Advanced Surveillance Technologies

Surveillance technologies aid in the monitoring of behaviors and communications of individuals and can be either overt (e.g. visible security cameras or disclosures of audio recording) or covert. Surveillance has several ethical issues that should be carefully considered including the *personal nature* of what is collected, whether the *goals* of the surveillance serve a larger pubic purpose (such as protecting public safety), and whether there are *alternative means* that are less intrusive to individual privacy which could accomplish the same outcome. [22]

Several frontier technologies will expand capabilities of governments as well as companies, NGOs, and individual citizens, to engage in surveillance activities. *Gigapixel Surveillance Cameras* incorporate high resolution cameras which can be attached to drones for high resolution photography from a distance. Japanese start-up Axelspace is building microsatellites are developing high resolution daily satellite imagery. Axelspace plans to sell access to an API which would allow any developer access to their imagery.[23]

Facial recognition software uses computer vision to identify the identity of individuals. Products utilizing facial recognition are being built for a broad range of private sector applications—from diagnosing children with autism, to assessing consumer interest in stores for targeted advertising, to expediting check-ins at airports, clinics, voting booths, and hotels.[24] Law enforcement agencies are a significant customer of facial recognition technologies as well. They leverage this technology to aid with the identification of suspects and arrests.

One subset of facial recognition, *emotion AI,* evaluates individual emotional states through facial expressions, gestures, voice tones, and other indicators to arrive at evaluations of emotional states including pleasure, anger, fear, or fatigue. The most common application of emotion AI is in advertising research to measure reactions to ads and social media content. Other applications of emotion AI are being developed for security screening, enterprise solutions software to monitor employees for 'emotional infractions' such as anger or not smiling at customers, [25] and to monitor customer service experiences in venues such as airports.[26]

Facial recognition has been one of the more publicly contentious of frontier technologies. Research from MIT has shown that facial recognition software misidentifies minorities at a rate higher than whites, for example.[27]

Governance of Surveillance Technologies

Existing governance of surveillance technologies is primarily carried out through a combination of export controls imposed by governments and monitoring by human rights NGOs. Electronic Frontier Foundation has proposed 'Know Your Customer' voluntary standards to help companies building technologies that may be utilized for surveillance understand and anticipate the intentions of potential customers.[28] Privacy International builds and maintains the Surveillance Industry Index (SII) which monitors the activities of surveillance equipment suppliers globally.[29]

There is an ongoing debate on the acceptable uses of facial recognition which has resulted in a number of legislative proposals in the U.S. These include a bipartisan bill in U.S. Congress, state bills in Washington and Massachusetts, and a proposed local ordinance to ban use of facial recognition technology by the city government in San Francisco.

Frontier Technology: Export Controls and National Security

The broad range of potential applications of frontier technologies has raised national security concerns for governments globally. In November 2018, the U.S. Department of Commerce proposed a review of a list of technologies for potential export controls. Among the technologies under review are AI, neurotech, quantum computing, genome editing, and a range of robotics and advanced materials.[30] Export controls could contain provisions on sales to foreign nationals and inclusion of certain nationalities in product development teams.[31]

The Committee on Foreign Investment in the U.S. (CFIUS), is an interagency authority with the power to review and block commercial transactions with a foreign entity or individual on concerns of national security.[32] Most CFIUS actions have focused on large telecoms and military equipment. In the last few years, the focus has expanded to a broader range of companies, including digital platforms like Uber and start-ups that hold consumer data that could potentially be used for manipulation and blackmail of U.S. citizens, such as dating apps with data on sexual preferences. CFIUS recently ordered PatientsLikeMe, a Boston start-up that facilitates patients sharing their medical information, to divest a $100 Million investment from Chinese genomics company iCarbonx. There are over $20 Billion in pending CFIUS divestment cases.[33]

Suggested Readings:

- Ranking Digital Rights: Investor Research Note: Poor Digital Rights Performance: Who Pays the Price? (Link)

Appendix SASB Software & IT Services: Sustainability Accounting Standard, SICS: TC0102

Full Definitions available at:

https://www.sasb.org/wp-content/uploads/2014/04/SASB_Standard_SoftwareIT_Provisional.pdf

TOPIC	ACCOUNTING METRIC	CATEGORY	UNIT OF MEASURE	CODE
Environmental Footprint of Hardware Infrastructure	Total energy consumed, percentage grid electricity, percentage renewable energy	Quantitative	Gigajoules, Percentage (%)	TC0102-01
	Total water withdrawn, percentage recycled, percentage in regions with High or Extremely High Baseline Water Stress	Quantitative	Cubic meters (m^3), Percentage (%)	TC0102-02
	Description of the integration of environmental considerations to strategic planning for data center needs	Discussion and Analysis	n/a	TC0102-03
Data Privacy & Freedom of Expression	Discussion of policies and practices relating to collection, usage, and retention of customers' information and personally identifiable information	Discussion and Analysis	n/a	TC0102-04
	Percentage of users whose customer information is collected for secondary purpose, percentage who have opted-in	Quantitative	Percentage (%)	TC0102-05
	Amount of legal and regulatory fines and settlements associated with customer privacy[9]	Quantitative	U.S. dollars ($)	TC0102-06
	Number of government or law enforcement requests for customer information, percentage resulting in disclosure	Quantitative	Number, Percentage (%)	TC0102-07
	List of countries where core products or services are subject to government-required monitoring, blocking, content filtering, or censoring[10]	Discussion and Analysis	n/a	TC0102-08
Data Security	Number of data security breaches and percentage involving customers' personally identifiable information[11]	Quantitative	Number, Percentage (%)	TC0102-09
	Discussion of management approach to identifying and addressing data security risks	Discussion and Analysis	n/a	TC0102-10

TOPIC	ACCOUNTING METRIC	CATEGORY	UNIT OF MEASURE	CODE
Recruiting & Managing a Global, Diverse Skilled Workforce	Percentage of employees that are (1) foreign nationals and (2) located offshore[12]	Quantitative	Percentage (%)	TC0102-11
	Employee engagement as a percentage[13]	Quantitative	Percentage (%)	TC0102-12
	Percentage of gender and racial/ethnic group representation for: (1) executives and (2) all others	Quantitative	Percentage (%)	TC0102-13
Managing Systemic Risks from Technology Disruptions	Number of (1) performance issues and (2) service disruptions; total customer downtime[14]	Quantitative	Number, Days	TC0102-14
	Discussion of business continuity risks related to disruptions of operations	Discussion and Analysis	n/a	TC0102-15
Intellectual Property Protection & Competitive Behavior	Number of patent litigation cases, number successful, and number as patent holder	Quantitative	Number	TC0102-16
	Amount of legal and regulatory fines and settlements associated with anti-competitive practices[15]	Quantitative	U.S. dollars ($)	TC0102-17

Endnotes

1 SASB. 2014. "Software & IT Services: Sustainability Accounting Standard, SICS: TC0102" https://www.sasb.org/wp-content/uploads/2014/04/SASB_Standard_SoftwareIT_Provisional.pdf

2 For most recent public opinion surveys on privacy see: "Online Privacy and Safety," *Pew Research* https://www.pewresearch.org/topics/privacy-and-safety/

3 For a review of U.S. state and federal regulatory proposals on privacy see: "Congress Begins Consideration of Comprehensive Federal Privacy Legislation," February 19, 2019, *Wilmer Hale* https://www.wilmerhale.com/en/insights/client-alerts/20190219-congress-begins-consideration-of-comprehensive-federal-privacy-legislation

4 "Twitter's Bot Problem Still Seems as Bad as Ever," 2018. *Vanity Fair* https://www.vanityfair.com/news/2018/11/twitters-bot-problem-still-seems-as-bad-as-ever?verso=true

5 "#Keepiton: What is an Internet Shutdown?" Accessed April 16, 2019 at: https://www.accessnow.org/keepiton/

6 "Investor Briefing: Stay Connected: Telecoms and the protection of human rights," *Fair Pensions*, 2016. https://shareaction.org/wp-content/uploads/2016/01/StayConnected2011.pdf

7 "The Global Network Initiative Principles." Accessed April 16, 2019 at: https://globalnetworkinitiative.org/gni-principles/

8 JUST Capital, Issues: Protects Customer Privacy," Accessed April 16, 2019 at: https://justcapital.com/issues/customers

9 "Ranking Digital Rights Index" Accessed April 16, 2019 at: https://rankingdigitalrights.org/index2018/

10 "The Transparency Reporting Index," Accessed April 16, 2019 at: https://www.accessnow.org/transparency-reporting-index/

11 "Asilomar Principles," Future of Life Institute, https://futureoflife.org/ai-principles/

12 "Ethics in Action," IEEE, Accessed April 16, 2019 at: https://ethicsinaction.ieee.org/

13 AI Principles of major technology companies include: Microsoft: https://www.microsoft.com/en-us/ai/our-approach-to-ai Google: https://ai.google/principles/ IBM: https://www.ibm.com/blogs/policy/trust-principles/

14 "Google AI Principles," *Google* Accessed April 16, 2019 at: https://ai.google/principles/

15 "IOT Number of Connected Devices Worldwide," *Statista* Accessed April 28, 2019 at: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

16 "2018 Roundup of IoT Forecasts and Market Estimates," 2018. *Forbes* https://www.forbes.com/sites/louiscolumbus/2018/12/13/2018-roundup-of-internet-of-things-forecasts-and-market-estimates/#394030227d83

17 Ibid.

18 Newman, Lily. 2017. "Medical Devices are the Next Security Nightmare." *The Atlantic* https://www.wired.com/2017/03/medical-devices-next-security-nightmare/

19 Ienca, Marcello, Pim Haselager & Ezekiel J Emanuel. "Brain leaks and consumer neurotechnology," *Nature Biotechnology* 36, s805–810 (2018) https://www.nature.com/articles/nbt.4240

20 "The Terrifying Potential of the 5G Network," 2019. *New Yorker* https://www.newyorker.com/news/annals-of-communications/the-terrifying-potential-of-the-5g-network

21 "Experts Worry 5G Could Widen Digital Divide," 2019. *The Hill* https://thehill.com/policy/technology/409047-experts-worry-5g-could-widen-digital-divide

22 "The Ethics (or not) of Mass Government Surveillance," Stanford Dept. of Computer Science, https://cs.stanford.edu/people/eroberts/cs181/projects/ethics-of-surveillance/ethics.html

23 "Axelspace," *Disrupt100* Accessed on April 28, 2019 at: http://www.disrupt100.com/?company=axelspace

24 "Like It or Not Facial Recognition is Already Here: These Are The Industries It Will Transform First," 2019. *CBInsights* https://www.cbinsights.com/research/facial-recognition-disrupting-industries/

25 For a review on U.S. workplace privacy practices: "Toolkit: Workplace Privacy," *Society for Human Resource Management (SHRM)* https://www.shrm.org/resourcesandtools/tools-and-samples/toolkits/pages/workplaceprivacy.aspx

26 Shell, Ellen. 2018. "The Employer Surveillance State." *The Atlantic* https://www.theatlantic.com/business/archive/2018/10/employee-surveillance/568159/

27 https://www.nytimes.com/2019/04/03/technology/amazon-facial-recognition-technology.html

28 "Know Your Customer," *Electronic Frontier Foundation*, Accessed April 16, 2019 at Ahttps://www.eff.org/deeplinks/2011/10/it%E2%80%99s-time-know-your-customer-standards-sales-surveillance-equipment

29 "Global Surveillance Industry," *Privacy International*, Accessed April 16, 2019 at https://privacyinternational.org/explainer/1632/global-surveillance-industry

30 "Department of Commerce Reviews Export Controls for Emerging Technologies," 2018. Accessed April 28, 2019 at: https://www.whitecase.com/sites/whitecase/files/files/download/publications/department-commerce-review-export-control-emerging-technologies-final.pdf

31 "Pro Rata: Top of the Morning," 2019. *Axios* https://www.axios.com/newsletters/axios-pro-rata-a39b3c29-e3d7-4c04-ba78-8c9ff282ea8e.html?utm_source=newsletter&utm_medium=email&utm_campaign=newsletter_axiosprorata&stream=top

32 "CFIUS." *U.S. Department of Treasury* Accessed on April 28, 2019 at: https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius

33 "The Trump administration is forcing this health start-up that took Chinese money into a fire sale," 2019. *CNBC* https://www.cnbc.com/2019/04/04/cfius-forces-patientslikeme-into-fire-sale-booting-chinese-investor.html