

# Opportunity and Hazard: 2020 and Beyond

A GROUPM PUBLICATION



APRIL 2019

group<sup>m</sup>

**GroupM**

3 World Trade Center  
175 Greenwich Street  
New York, NY 10007  
USA

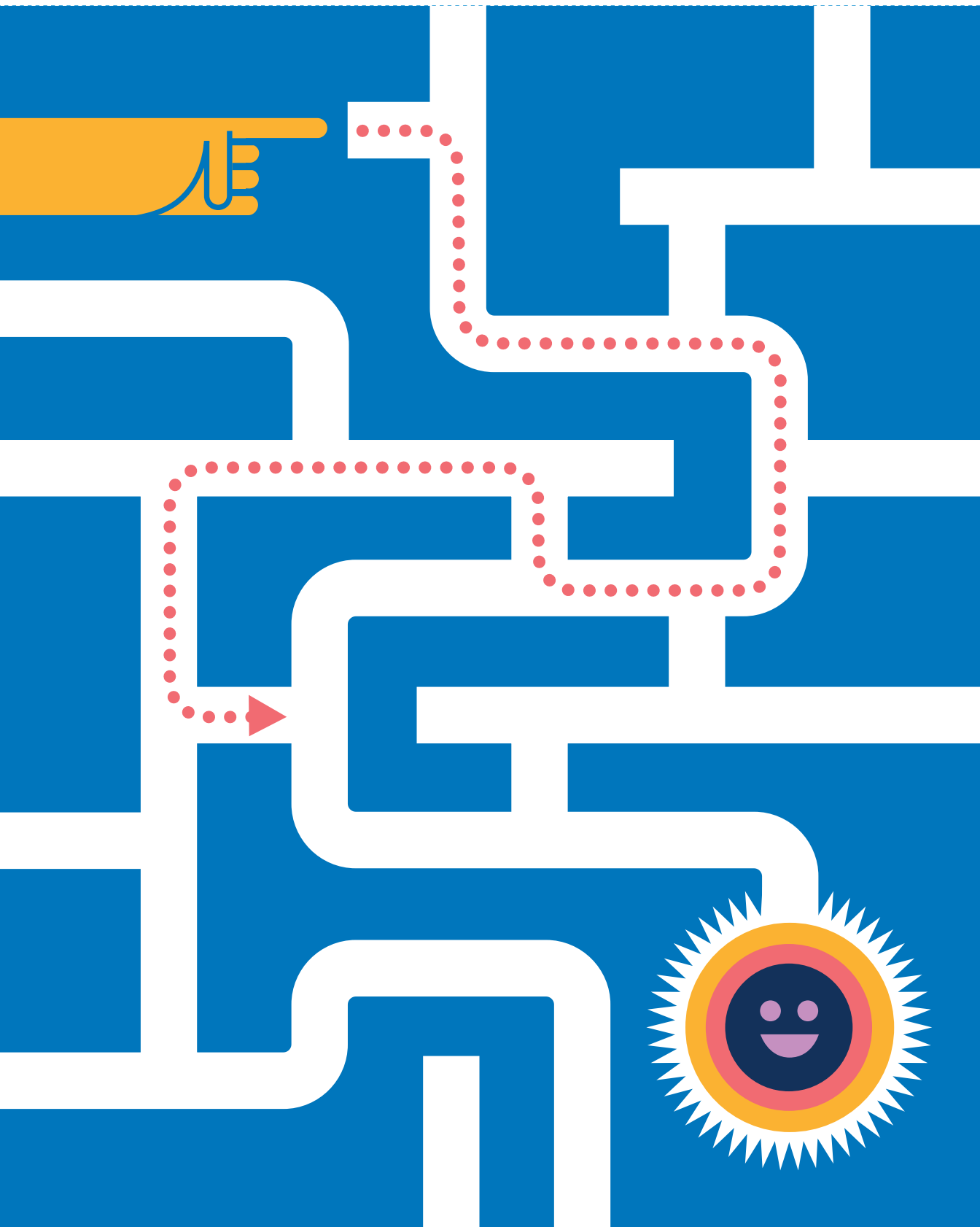
All rights reserved. This publication is protected by copyright. No part of it may be reproduced, stored in a retrieval system, or transmitted in any form, or by any means, electronic, mechanical, photocopying or otherwise, without written permission from the copyright owners.

Every effort has been made to ensure the accuracy of the contents, but the publishers and copyright owners cannot accept liability in respect of errors or omissions. Readers will appreciate that the data is up-to-date only to the extent that its availability, compilation and printed schedules allowed and subject to change.

# CONTENTS

GROUPM: THE DRIVERS OF CHANGE FOR THE NEXT DECADE . . . . .	4
THE VALUE OF EVERYTHING, THE PRICE OF EVERYTHING . . . . .	6
5G – 2019’S WISHFUL THINKING, 2022’S REALITY . . . . .	9
AI – THE KILLER ROBOTS CAN WAIT. . . . .	13
THE AGE OF ASSISTANCE AND LIFE AFTER THE SMARTPHONE? . . . . .	19
IDENTITY . . . . .	24
PRIVACY . . . . .	29
BRAND AND SOCIAL SAFETY . . . . .	35
DIRECT BRANDS . . . . .	38
A LAST WORD . . . . .	42
APPENDIX . . . . .	44

# GROUPM: THE DRIVERS OF CHANGE FOR THE NEXT DECADE



# GROUPM: THE DRIVERS OF CHANGE FOR THE NEXT DECADE

Welcome to GroupM's perspective on some of the foundational technologies likely to effect changes in consumer adoption of products and services. In our commentary (not prediction), we try to err on the side of the likely and focus on areas that will require some change to the medium-term planning horizons of brand owners and content creators. Many of these issues will be familiar to readers, though our interpretation may be met with enthusiastic disagreement from partners, clients and colleagues. As always, we welcome comments and contributions as to how we should think about the future state of the world, and our business of demand generation and optimization within that world.

This paper covers new developments in the areas of bandwidth, the increasing "intelligence" of machines, the concept and application of identity, and the possibility of life after the most successful consumer product in history — the smartphone. We also touch on issues of privacy and "brand safety," and in doing so recognize that we are comingling the objective and subjective and that our view will be somewhere on the continuum that our clients, partners and regulators must consider. Finally, we comment on the rise of "Direct Brands," which represent a new category of enterprise enabled by technology and data, and that are now a threat to the profitability of legacy brand owners. There is no comment on blockchain, which is the subject of another GroupM piece that was recently published.

In the autumn of this year, GroupM will publish its observations on the world's biggest, most progressive and most influential companies in the fields of media, entertainment and commerce. By that time we will know the first steps of Disney+, AppleTV+ and NBCU's new streaming services, together with the response from Netflix and Amazon. The direction of Sky under Comcast ownership will become clear, as will AT&T's plans for Warner Media, to say nothing of its vision for the future of advertising.

We will also be able to measure the public's appetite for media subscriptions as pay walls rise and OTT channels proliferate. The consolidation of ad tech will have progressed. Regulatory scrutiny of major platforms may have taken a significant turn, Pinterest and others will likely be publicly traded, eSports will continue its surge into marketer consciousness, and so it will continue. Perhaps most interesting of all will be to track the progress of Instagram as a commerce platform and Google's gaming ambitions as both seek to diversify revenue streams. Our goal will be to map the opportunities and threats for advertisers as the decade turns.

It may also be time to review the impact of legislation: in particular, Articles 11 and 17 of the new EU Copyright Directive. These allow publishers to charge for news snippets and place the burden on the platforms to find and remove copyrighted material posted without authorization. This may be the prelude to wider demands for "pre-detection" exclusion. This constitutes an existential threat and also a new world order of an American wide web, a European "not so" wide web and a Chinese "very narrow" web. This paper is not an analysis of all the market protagonists, nor is it a comprehensive survey of recent events and regulations. Hopefully, though, it will be thought-provoking and impartial to the extent that opinion can be.

# THE VALUE OF EVERYTHING, THE PRICE OF EVERYTHING



# THE VALUE OF EVERYTHING, THE PRICE OF EVERYTHING

---

Oscar Wilde's character Lord Darlington said that a cynic is "a man who knows the price of everything and the value of nothing." The disturbing truth is that throughout history, particularly as it relates to technology, many things have value and everything has a price.

Today that remains the case, but the difficulty of forming a judgment is compounded by the velocity of change, the velocity and volume of commentary (the irony is not lost on us), liberal disregard for facts or for proportionality, and the conflation of issues to suit the purpose of either proponent or opponent. There is no supply-side crisis of opinion.

It's fair to say with some degree of detachment, however, that many of today's developments have "succeeded" in triangulating widely distributed human progress with narrowly captured economic benefits and the ability of bad actors to weaponize the exact technologies that create the benefit for others. For regulators this is a Bermuda Triangle in which policy becomes mangled by contradiction.

"Smashing the machines" is no more an option now than it was in the cotton towns of early 19th century Britain. The Luddites (now a catchall for those opposed to progress through technology) were, in fact, a society of textile workers dedicated to destroying the machines that were subverting the traditional relationship between capital and labor in "a fraudulent and deceitful manner."

Now, as then, the solution is elusive. General progress has never meant universal progress, nor anything that resembles equality of opportunity. The trade-offs have always been epic and troubling: prosperity in exchange for climate change, genetic engineering and industrial scale farming in exchange for famine elimination.

A further complication is that the new order has little respect for old constructs like national borders and language. Advances in technology today almost always lead to a reduction in friction and the creation of network effects amplified by the zero-transport costs of data. What were the odds of streaming music being dominated by a Swedish start-up, of Netflix successfully pivoting from renting DVDs through the mail to streaming in over 190 countries, or of a search start-up becoming the most valuable company in the world in 20 years from launch? None of them had any lock on natural resources, nor did they benefit from allocation of spectrum or other resources, and thereby achieved terrific market power without any obvious regulatory counter-leverage. What governments do not give, they find problematic to take away.

In circumstances such as these, regulation (or forced breakup) is a complex business that's fraught with risk. Often the easiest targets for regulation are those that are least able to defend themselves. They are most likely to be unable to execute a workaround and thus abide, assuming survival, by the rules. The early actions under Europe's General Data Protection Regulation (GDPR) may enfeeble the small

What  
governments do  
not give, they  
find problematic  
to take away.

# THE VALUE OF EVERYTHING, THE PRICE OF EVERYTHING

---

Many believe  
the personal  
value of these  
companies  
outweighs any  
collective social  
cost.

and further empower the mighty. Additionally, the biggest targets are also the ones that provide the greatest utility to the greatest proportion of the population. It's interesting to note that despite huge press and parliamentary protestation, the economic performance of Facebook, Google and Amazon (under less scrutiny) has barely missed a beat. There are some who ascribe this to a Faustian bargain at unimaginable scale. In short, in any practical sense, many believe the personal value of these companies outweighs any collective social cost.

The next decade could be even more dramatic than the last. Change is the only certainty, but it seems clear that the ethical and social ramifications of that change will be as important as the economic implications that typically concern advertisers and their fellow travelers.



# 5G – 2019'S WISHFUL THINKING, 2022'S REALITY



# 5G – 2019’S WISHFUL THINKING, 2022’S REALITY

---

It’s possible that the upgrade to 5G may be the most significant enabling event in the brief history of the internet.

It’s been 25 years since cover-mounted silver AOL discs provided the first populist gateway to the internet and the world wide web. That was a period when demand for bandwidth far exceeded supply, to the extent that users were happy to pay by the minute. A generation later, we pay a high price for fixed wire access — often to local monopolies or on a metered basis — to what we still call mobile carriers. In fairness to all, the cost per megabyte of data has fallen at a geometric rate, and today’s commonplace notions like 4K streaming were considered fanciful a quarter of a century ago (assuming they were contemplated at all). Perhaps most remarkably from a global perspective, the cost of a gigabyte of mobile data to a consumer in India is now lower than it is to people in the United Kingdom and the United States.

The future promises something different altogether. Bandwidth will be unconstrained by speed and capacity, and it will be funded not just by consumer and business communications and content, but by the commercial application of IoT and the proliferation of smart speakers, smarter cities and autonomous vehicles. We have great expectations.

We are entering the fourth age of connectivity. Dial-up was first (it enabled communication), then fixed-wire broadband from ADSL to fiber (which enabled content and commerce), then mobile broadband via 4G LTE (which enabled an untethered world), and now 5G. Several years ago, we posited that the transition from dial-up to broadband was bigger than the change from no internet to dial-up. It’s possible that the upgrade to 5G may be the most significant enabling event in the brief history of the internet. (It’s important to note that there is no significance to the letter “G.” The 5G infrastructure is entirely new and not an iteration of what went before.)

5G, the next-generation mobile framework, will start to roll out in 2019. It will set new expectations of opportunities to advance the way we interact with each other, and with both our communication and content choices and the built environment. Simply put, 5G is a new set of rules and standards that guide smartphone manufacturers and network operators to create a more efficient mobile experience.

The central concept is that creating additional direct connections to the end servers (by implementing a network of small cells) will increase upload and download speeds dramatically. Leading chipmaker Qualcomm has measured max download speeds of 4.5gb/s at peak performance, though it expects typical speeds to be around 1.4gb/s in the early stages of the rollout. As an aside, 1.4gb/s is one hundred thousand times greater than a 14.4 kb/s dial-up modem. So it’s no surprise that latency — the delay before a connection is made with the server — would also nearly disappear under the new framework.

As a result, the marginal cost of bandwidth required to stream or download a movie via 5G will be negligible compared to its predecessor. This will create the opportunity to add additional devices onto mobile networks without compromising the efficiency of the network, solving

# 5G – 2019’S WISHFUL THINKING, 2022’S REALITY

the issue of contention that’s familiar to anyone who has attempted to post a video in a full stadium.

Proponents of 5G claim that the new technology will usher in a perfectly connected world. Inevitably, media consumption is expected to continue to climb as users stream high-quality video on the go and when the linear relationship between data consumption and cost is broken. The increase in available bandwidth likely will be an accelerant of both augmented and virtual reality technologies and applications as well. In part at least, this will be enabled by shifting much of the processing power from the headsets to offsite servers, allowing manufacturers to create more attractive devices.

In a 5G world, anything that can be connected to the internet will be. This interconnectedness is everything. A single smart refrigerator is of limited use; a smart refrigerator that connects with the prosaic (auto-refill shopping lists) and the life-critical (health monitoring ecosystems) creates new commercial and social opportunities. 5G represents the real dawn of device-to-device networking.

The data exhaust generated by activity in a 5G environment will be a substantial driver for the advancement of artificial intelligence; the more data an algorithm can analyze, the more it can predict future results. In turn, this is a precursor to the large-scale deployment of autonomous systems, particularly in sectors where the autonomous and analog coexist. Most of the technical challenges of autonomous vehicles have been solved by engineering and deep learning systems. The remaining challenges are very human: those of ethical judgment and the interaction between the autonomous and the slower-to-evolve human vehicle operators.

## Commercial and technical hurdles

While there will undoubtedly be positive advancements from the rollout of 5G, they won’t come without a cost. With the repeal of net neutrality rules in the United States, it is possible that infrastructure providers will offer discriminatory pricing structures and constrain the speeds of the biggest users of data. From the consumer perspective, there will also be a need to purchase new smartphones to access cellular services, and new home appliances if they want to take full advantage of the connected world. It is possible that each device will need its own data plan, much like buying a cellular-connected iPad or Apple Watch today. We may even be reaching an uncomfortable tipping point at which fear of obsolescence challenges the desire for the incrementally smart: “My refrigerator still chills well but won’t talk to Alexa. Decisions, decisions.”

Other impediments to early adoption of the new technology will result from an uneven pattern of availability within individual markets. While each telecom and infrastructure company is pursuing its own rollout strategy, coverage is not expected to be ubiquitous under any provider for at least a few years. In the United States it took several years before

“My  
refrigerator  
still chills  
well but won’t  
talk to Alexa.  
Decisions,  
decisions.”

# 5G – 2019'S WISHFUL THINKING, 2022'S REALITY

---

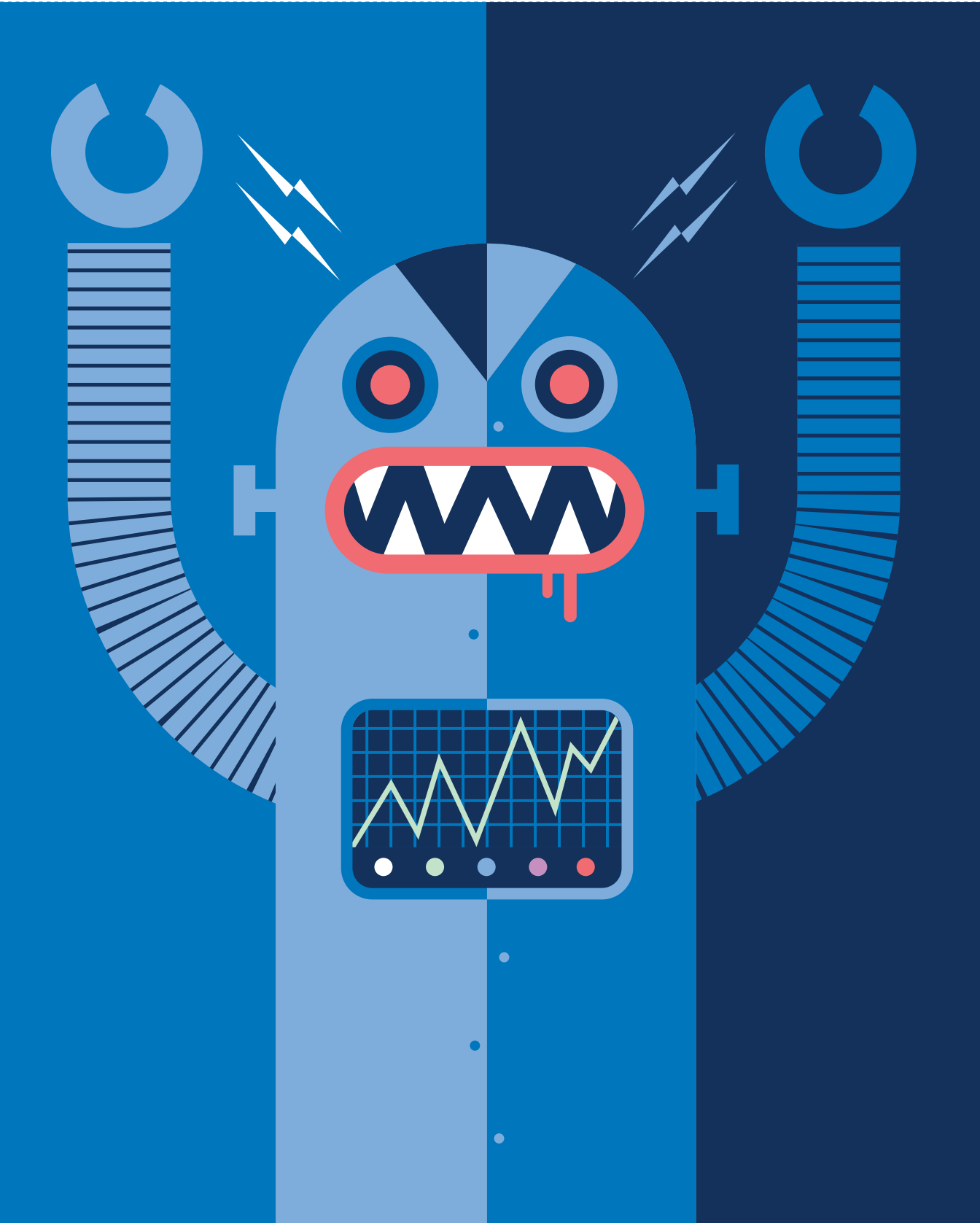
Smartphone makers have never been more anxious for a technology step change that reinvigorates device demand.

4G LTE became fully accessible nationwide, and it is likely that 5G will take longer. Even the technical specifications are inconsistent across providers. The millimeter wavelength network being implemented by Verizon would be optimal for cities, as the range for each small cell is limited. However, it's not clear if the signal will be able to penetrate walls, particularly in older buildings. Sprint, by contrast, will use mid-band spectrum to deliver a version of 5G that travels farther but at lower speeds. The worst of all scenarios is a return to the days when competing standards like GSM and CDMA (like VHS and Betamax before them) forced consumers to make choices that had little to do with utility.

There are also real and perceived health, safety and privacy concerns that may slow the adoption of 5G. Some municipalities have already decided that they will not install the small cells out of concern that they may cause cancer. Others have balked at the breadth of the data that will be passing through the networks and how it can become a vulnerability that can be exposed not only by criminals, but also by foreign governments as an act of cyberwarfare. There have already been allegations that China's Huawei may have used its networking hardware to spy on its citizens and foreign governments. Huawei's exclusion has knock-on economic consequences; Vodafone said in March that the cost would be hundreds of millions of dollars and a significant delay in the roll-out of 5G in the UK.

All that said, smartphone makers have never been more anxious for a technology step change that reinvigorates device demand. It will be interesting to see whether network capability or new form factors (like foldable devices) will be the bigger driver.

# AI – THE KILLER ROBOTS CAN WAIT



# AI – THE KILLER ROBOTS CAN WAIT

---

Today, we have a near unimaginable abundance of computing power.

In the 1950s, pioneers of AI sought to replicate human intelligence in machines. There were two primary avenues: rule-based AI composed of “if X then Y systems,” and neural networks that tried to mimic the way humans learn. The two main components required for neural networks were data and computing power. These were not strong in the 1950s, the deficit remained through the pre-silicon age, and by the 1980s neural networks had taken a back seat to rule-based systems.

Today, we have a near unimaginable abundance of computing power. It’s sobering to think that the moon landing 50 years ago was achieved with one thousandth of the on-board computing power of the first iPhone. Now we are witness to a confluence of excellence in computer science, engineering and neuroscience that has created fertile ground for huge advances in neural network-based machine and deep learning. The final ingredient is massive amounts of data from which the machines can learn. A search for the “winners” might start with a useful equation:

DATA VOLUME X SOURCES OF SIGNAL X AVAILABLE PROCESSING POWER = LEADERSHIP

In his book “Architects of Intelligence,” Martin Ford offers a useful primer on how AI systems learn. We paraphrase it here:

**SUPERVISED LEARNING** accounts for 95 percent of practical AI systems. The machine is trained with vast amounts of structured, labeled data. A million pictures of dogs labeled “dog” will pretty much ensure the machine’s ability to recognize the next dog. The same basic rules apply in translation and medical imaging. It’s the massive data visibility that Google, Facebook and Amazon have that creates competitive advantage in this area.

**REINFORCEMENT LEARNING** is learning by trial, error and reward. The machine is presented with a problem that it seeks to solve itself. Each time it succeeds that success is baked into the algorithm, and this is iterated to a successful outcome. While supervised learning needs massive data, reinforcement learning needs massive capacity to deal with the instances of failure that precede success.

**UNSUPERVISED LEARNING** is something of a holy grail because it’s how humans learn using observation and experience that lead to context. To date there are no “in the field” examples of unsupervised learning. (The gap between human and machine behavior is continually reinforced by the “ingenuity” displayed by bad actors in gaming and defeating the efforts of Facebook and Google to keep themselves safe for users and advertisers.)

To some, the end game is artificial general intelligence (or even superintelligence) in which the functioning of machines would only be distinguished from human function by their reliability and, in the end, superiority.

# AI – THE KILLER ROBOTS CAN WAIT

---

In an abstract sense the world is ready for artificial intelligence. That's especially true when to most people the real-life manifestation of AI is computers that are good at games, and when AI and sci-fi have converged in popular culture.

In some ways we reached a mountaintop of reinforcement learning when DeepMind's AlphaGo conquered the world's most complex game. In the grandest yet simplest terms, we are watching a key development from machine learning to learning machines.

We are in the land of neural networks iterating through back propagation and making sense of unstructured and often unlabeled data. We are still between a decade (maybe) and a century (way more likely) from the development of artificial general intelligence, and thus can restrict our fear and ambition to that presented by human and corporate actors. The killer robots can wait. In the meantime, business leaders and regulators don't need to simply understand how to discover new technology, but how to apply the right (in every imaginable sense of the word) technology in the right situation.

AI will accelerate capability gaps within and between companies, sectors and countries as the data-rich become the AI-rich who will operate on accelerated cycles of innovation. More high-quality data fuels AI and produces better products, increases traceable customer interactions, and produces still more and better data. Amazon Go's staff and checkout-free stores are the product of verified identity and supervised learning that informs smart cameras. Increasingly, the aggregated signals from all Amazon interactions will boost the relevance and efficiency of the next transaction made.

There is a truth about AI and enterprise: Entities that see and capture the most relevant data will win. The question is whether they will win in a:

- Narrow application — every brain scan ever made or every online ad served.
- Broader application — everything anyone ever bought or watched.
- Broadest application — everything anyone ever said or did and every place they went.

In the West there will be multiple winners in narrow AI, like IBM in medical imaging perhaps or Google and The Trade Desk in programmatic advertising delivery. In broader terms, particularly as it relates to commerce, Amazon is a clear leader. In business operations Microsoft may be the same, as the two Seattle giants crunch ever bigger data sets in the AWS and Azure clouds.

The most broadly defined application — understanding human behavior and emotional states — creates the most unease. Here, Facebook and especially Google are way, way ahead. Both companies know more about

In an abstract  
sense the  
world is ready  
for artificial  
intelligence.

# AI – THE KILLER ROBOTS CAN WAIT

---

AI will create a landscape of ethical complexity for which we may be poorly prepared.

their billions of users than is known by friends, family, lovers, employers and governments.

What makes Google (and Amazon) especially interesting is that, in contrast to their walls around reach and frequency data, their cloud services businesses increasingly offer “open source to go.” Consequently, in creating new knowledge of their own, thousands of businesses are increasing the knowledge of Amazon and Google. They are not alone. In China, Alibaba and Baidu lead AI development and implementation.

We remain in the age of discovery for AI, but also in a time of its practical application to problems as diverse as health care and transportation. Just as significantly, AI will create a landscape of ethical complexity for which we may be poorly prepared. The most commonly discussed ethical use case surrounds decision-making by autonomous vehicles. If a vehicle sees a child in its path and has enough time to swerve but not to stop, how does it trade injury to the child against possible injury to people in other vehicles or on the sidewalk? Ethics also play a part in managing both conscious and unconscious bias in decisioning over the provision of services like health insurance and activities like social resource allocation. In short, AI has the potential to widen the digital divide and accelerate social inequality as well as the chance to be a driver of significant positive change and societal benefit.

AI, certainly to the extent of machine learning applications, has become almost commonplace in marketing and advertising:

- The sophistication of search engines makes them unrecognizable from a decade ago. Their predictive capabilities and use of image and speech recognition have transformed the experience.
- The same underlying techniques, combined with filtering and sophisticated cluster analysis, have done the same for predictive content recommendations in media and e-commerce applications. The same is true for “personalized” advertising and customer service delivery.
- Speech recognition and natural language processing enable chatbots, so-called “conversational” AI, and sophisticated sentiment analysis.
- Areas such as dynamic pricing — which have long existed, most notably in airline ticketing — are becoming pervasive as crawlers learn more about competitive pricing and the price sensitivity of different customer cohorts.
- The efforts of Google, Facebook, Twitter and others to police the exponential proliferation of content and comment require incredible resources. They have come a long way, but not far enough.



# AI – THE KILLER ROBOTS CAN WAIT

---

The common factor is scale and speed at orders of magnitude that are replicable only by the tiniest subset of advertisers.

We should be careful to distinguish the automated and even the algorithmically informed, of which there are a lot, from the autonomous, of which there are few. Those that have begun to deploy autonomous systems face an unexpected challenge: explaining how it works, not just demonstrating that it works. Furthermore, autonomous systems that cross long-established silos can prove challenging to the prospective buyer. It's equally useful to distinguish between predictive systems that look back to forecast a future state and prescriptive systems that will recommend next actions. The marketing industry and its supply chain will need to reorganize around the data of tomorrow rather than around the channel silos of today.

Transacting media is an activity that obviously will benefit from machine and deep learning. It represents an immense data set and a near infinite range of outcomes. It defies precision and predictability in the hands of humans. The machines are doing better and will do better still; even here ethical issues will arise, as it's far from impossible that brand owner A could learn enough about brand owner B's strategy to gain competitive intelligence. It's even more likely that AI will create targeting decisions that discriminate in areas of age, gender, race and location, or worse, prey on addiction, depression or other afflictions.

AI has  
become almost  
commonplace in  
marketing and  
advertising.

# AI – THE KILLER ROBOTS CAN WAIT

## AI and China

In Kenneth Pomeranz's book "The Great Divergence," he refers to the process through which the Western world overcame premodern growth and overtook empires such as China. Consider global GDP. Up until the 1750s, China dominated and dwarfed India and the imperialist powers of Northern Europe. This only changed with the advent of the industrial revolution in western Europe in the early 19th century and decades later in post-Civil War United States. This was the catalyst for the great divergence between the West and China. Some of the most important inventions of any age — including the compass, gunpowder and printing — came from China, but industrialization did not follow. In the last 25 years China has, of course, industrialized up to and beyond any other nation, but success in the development and application of AI can potentially aid China in creating a new generation of economic leadership. The Chinese have typically taken the long view, and many believe the last 200 years have been an anomaly.

The availability of data in vast quantity alone is likely to support the Chinese endeavor.

Data can be assessed based on breadth (quantity of data, how many individuals), quality (structure and labels of the data) and depth (the number of data points about each user). Surprisingly, the breadth of data from China and the United States is about the same; although the Chinese population is larger, American companies pull data from across the globe. Depth of data may tell a different story.

To paraphrase remarks made late in 2018 by Kai-Fu Lee, chairman of Sinovation:

Chinese internet users channel a much larger proportion of their daily activities, entertainment, transactions from shopping to loans to payments of every kind, and interactions from messaging to ride-hailing loans to ride hailing through their smartphones — and often through a single platform like Alibaba and Tencent. Consequently, the ability of AI to observe and anticipate behaviors rises significantly.

The Chinese have developed a powerful iterative method of business innovation based on massive amounts of data in a highly competitive market where players don't mind occupying the same space. Chinese VCs also surpassed the U.S. in 2017 as the greatest investors in AI technology, making up 48 percent of global investment in AI. Additionally, the expectation of privacy is severely limited in China, allowing companies to use more sensitive data to train AI algorithms more quickly and to be more effective. As China expands its internet model and networking technologies to other countries, as it already has in Vietnam and Tanzania, it gains access to new data to fuel its algorithms. To China, the arms race in 5G is just as much about gaining access to data as it is about creating a new revenue stream.

If China is successful in expanding its internet model, it is likely that it will gain an early advantage in AI, and as a result, Chinese firms will reap the lion's share of funding. If this happens, it will be difficult for Western companies to compete with not only the breadth of data that China has access to, but the depth and the quality as well. There is no sign yet that the ambitions of the Chinese leaders are being hampered by consumer privacy and other data use restrictions, but tolerance for the possibility of unfettered capitalism may be tested soon.

# THE AGE OF ASSISTANCE AND LIFE AFTER THE SMARTPHONE?



# THE AGE OF ASSISTANCE AND LIFE AFTER THE SMARTPHONE?

---

It has taken more than 30 years to get from the mouse to widespread voice-activated human-machine interfaces.

Advancements in 5G, AI and fast-developing ecosystems of smart objects herald a generation shift in human-technology interactions. It is worth considering whether these new advances will ultimately lead to the death of the smartphone.

In 2007, Steve Jobs boldly declared that Apple was launching an “iPod, a phone, and an internet communicator.” Of course, this ended up being the first iPhone, and the rest is history. Humans, machines and human-trained machines have taken the smartphone from a two-dimensional utility to three dimensions and beyond. Today, smartphones are still used for communication, entertainment and information (a modern reworking of Jobs’ trifecta), but we are starting to extend to use the smartphone as a gateway to augmented reality and dedicated digital assistants. This new capability, when untethered, may be what begins to drag us from our smartphones to something else.

Most easily, this new age might be referred to as the Age of Assistance — not assistance narrowly defined by “voice” or by Hey Google, Alexa and their chums, but assistance defined as broadly distributed active, passive, anticipatory and timely responsiveness. Some of these forms of assistance will be useful but prosaic like some Alexa skills today, but others will be genuinely life-enhancing and even life-saving. That said, it’s quite remarkable that it has taken more than 30 years to get from the mouse to widespread voice-activated human-machine interfaces.

At last it seems like a real dividend might soon be paid back to society in the form of increased efficiency of time and energy utilization, improved public health, and safety from diagnostics and accident prevention. IBM, AT&T and Samsung triangulated a location-aware network, smart cameras and cloud processing to do just that. Maybe we will also see a reduction of waste through better preservation of food and other commodities, together with better optimized replacement cycles. All this from smart homes and cities, featuring connectors between people, objects and the surrounding physical environment.

It’s not possible to call the winner in the assistance race, as it seems likely that devices will, as a standard, be assistant agnostic. It’s hard to imagine an Alexa user buying a device that only responds to Bixby, Samsung’s proprietary helper. It’s also worth noting that while Amazon Echo’s Alexa is the leader in smart speaker sales, Apple’s Siri and Hey Google benefit from massive penetration of existing device ecosystems. At present, in consumer markets at least, Amazon and Google would appear to be the best positioned, as their assistants connect people to goods, services, entertainment, information and the plethora of small tasks and interdependencies that make up anyone’s life.

When Facebook became a commercial entity late in the last decade, Mark Zuckerberg coined the expression “social by design.” By 2021 we can expect “assisted by design” to be utterly pervasive. Sensors will keep us in the correct lane. Cameras will monitor foot-traffic congestion

# THE AGE OF ASSISTANCE AND LIFE AFTER THE SMARTPHONE?

by aisle. Data embedded in packaging will assist us simultaneously in recipe planning, health advice and shopping, by connecting to our health apps, refrigerators and calendars. Two years is enough time for every pack of every product, for every garment, and for every service to add assisting and discoverable data. This represents a considerable opportunity for the marketer that can be simultaneously transparent and more frequently relevant and valuable. For those that can't, consumer expectations may be hard to meet.

In this paper, we have not emphasized the implications for autonomous vehicles. Within three years, many vehicles will be semi-autonomous and deploy any number of driver-assist features. We expect there to be almost no vehicles on public roads that will be technically (and more important, legally) operating without human oversight. It's only when that happens that a societal rethink of the transportation experience will become relevant to most people and, by extension, most marketers.

The assisted, augmented life is not without societal risk.

The assisted, augmented life is not without societal risk.

2018 was technology's "annus horribilis" from the standpoint of damaged corporate and sector reputations arising from public safety, manipulation of platforms by bad actors and serial data breaches. There was no "ethics booth" at CES in January, but there is a growing need among market participants, including governments, to demonstrate that there is a strong social responsibility dynamic influencing how people think and apply applications of every kind.

Decoupling the core functionalities could also offer a way to provide these services to emerging markets and less wealthy populations. Instead of having to purchase an expensive smartphone, perhaps less expensive digital assistants could leverage public Wi-Fi or 5G networks and provide a basic means of communication and information-gathering to these populations. The impacts of this could be astronomical in nature. Entire populations that have been left behind by the digital age could take steps toward catching up with the rest of the world. Businesses and education could be bolstered by allowing access to the most recent and relevant information. Plus, massive amounts of net new data will be generated as these populations become connected to the internet.

One major challenge, however, is determining how the different services engage with one another. Today, iPhone users have a plethora of apps, all approved by Apple and organized into the App Store, which requires that all developers follow a strict set of rules to have their apps featured. These guidelines provide a common framework and a degree of security through the standardization process. Android has a similar setup through the Google Play store. If consumers shift away from

# THE AGE OF ASSISTANCE AND LIFE AFTER THE SMARTPHONE?

---

Less than 20 percent of WeChat's revenues arise from advertising sales. Facebook would welcome such diversification.

smartphones, it is unclear what the ecosystem will look like, and how the different apps or ecosystems will engage with each other. Will users still reap the benefits of being within one ecosystem or another, such as paying with Face ID or content syncing on their devices, or will users need to authenticate each device and service separately? Today, nearly all wearable technology is synced through smartphones in a personal area network (PAN). Perhaps as computing power increases and the processing power of smaller devices skyrockets, there will no longer be a need for a smartphone to act as a hub and the PAN can be managed through a smartwatch or another device.

The notion of a PAN is reinforced by a few concurrent developments. Tencent's continued integration of multiple services inside the WeChat app, and Facebook's back-end integration of Instagram, Messenger and WhatsApp may be key pointers. In the case of Facebook, the fusion of its three core messaging platforms — partly in the name of privacy and security — might also be a barrier to regulation and a breakup of its assets. It's instructive to know that less than 20 percent of WeChat's revenues arise from advertising sales. Facebook would welcome such diversification, as other elements of its monetization receive rising criticism.

In both these cases we are seeing the development of ecosystems, or even new operating systems, that seem to be agnostic to and perhaps ultimately independent of iOS and Android. Strategy consultancy Activate foresees a future in which messaging applications will integrate all of personal and enterprise messaging, commerce, payments, the gig economy, audio, video gaming and smart-home control. If this proves accurate, it will be a seismic disruption in the communication market structure and a major new consolidation of power.

At the market inception of mobile telephony (that's all it was) you chose your carrier first, your plan second and your device third. There were momentary disturbances in the force. There was a moment in America when desire for the StarTAC flip phone jumped the structure, and another when the Razr was the must-have device. Not until the iPhone, however, did the device become the most significant driver of choice. Now that has changed; you are an iOS person or an Android person. Thus, the OS sits atop the market structure, with carriers and devices below. Now we see the first sign that OS, carrier and consolidated multifunctional device-agnostic services may be getting us ready for life after the familiar form factor of portable screens.

# THE AGE OF ASSISTANCE AND LIFE AFTER THE SMARTPHONE?

---

It seems that the last hurdle to smartphone independence is a different construct of how we think of screens. There are several indicators of change:

- The rising penetration of smart speakers and embedded assistance in multiple devices.
- The cost of thin, foldable or bendable displays enabling seemingly endless amounts of surfaces to be activated as “screens.”
- Untethered connected devices like the Apple Watch.
- AR and VR hardware becoming smaller on the one hand and ubiquitous on the other, driven by AI development that aids the creation of more immersive experiences.

In aggregate, these changes may encourage consumers to leave the smartphone behind in favor of a combination of wearables and screens that become personal and responsive in the built environment. It’s philosophically interesting to note that “glasses” in any historical context have been used to correct nature’s faults. In the future they could enhance nature in a far more general sense.

It would be fanciful to describe the above scenario as “real and imminent” for all but the wealthiest sliver of the population. For most people, iOS devices are out of reach. Forget exotic digital eyewear — it will take the equivalent of a \$50 Android for the world at large to take a “magic leap.” Marketers are rightly cautious of the opportunity cost of focusing on subsets of subsets.

Changes may encourage consumers to leave the smartphone behind in favor of a combination of wearables and screens that become personal and responsive in the built environment.

# IDENTITY





Marketers have always believed their products and services — or the messages associated with them — were disproportionately important to some consumers over others. Put in context of a near-universal business goal of improving revenue while controlling costs, we can see the spirit behind targeting. For most of them, some form of targeting has always taken place, powered by information about consumer identities in the possession of either the media owner or the marketer, translated into trading segments that attempted to balance precision with scale, and mindful that customers often had characteristics that differed from a given media target.

To illustrate how approaches have evolved over time, consider that Ladies' Home Journal was founded in 1883, and presumably was helpful in reaching a higher skew of women rather than men. Age-based targeting was present at least as far back as the 1950s in print and the 1960s on television. Direct marketing via mail and telephone took off shortly thereafter, with the term itself coined by Lester Wunderman in the late 1960s. Lists of consumers, their addresses and other data became available from third parties around the same time. The goal of reducing wasted spending was usually a primary objective, but so too was customizing a message for different audiences. Marketers' capacity to manage data through computing power about their known customers or prospects steadily improved such that early customer relationship management (CRM) systems existed by the 1970s, which could help segment customers further based on bespoke characteristics. This continued more recently with the rise of the internet — especially with email, but also in other environments, using cookies and device IDs as proxies for individuals. Data management platforms (DMPs) assign audience characteristics to groups of cookies or device IDs, allowing them to be used in media buying. This, along with prophecies of the emergence of addressable advertising on television, continues to elevate interest in targeting and audience segmentation opportunities.

Moreover, many of these concepts have evolved to a point where they have converged. For example, CRM systems host email addresses — arguably the most important unique identifier most marketers have about most of their customers. It's an identifier that can be matched with third-party information about those known customers. Those data are now commonly used to target people individually on granularly assembled mass-reach media platforms, as with Facebook's Custom Audiences, Google's Customer Match and Twitter's Tailored Audiences, among other products. These data are amplified by the notion of the look-alike audience, and the capacity to infer characteristics of identity on a much wider segment of the population has become a reality. Of course, those inferred characteristics might lead an advertiser to target a male when they wanted a female, an older person when they wanted a younger one, or (at maximum irritation) someone who just bought the product and who won't buy it again for another 10 years. As with most things in advertising, it's not whether the solution is good or bad — it's whether it's better than the next-worst alternative. Contrary to

As with most things in advertising, it's not whether the solution is good or bad — it's whether it's better than the next-worst alternative.

# IDENTITY

---

Marketers may need to set their expectations lower in terms of how much personal information they should expect to gather about customers and prospects.

the narrative of many market participants, targeting is not a matter of binary truth; it's a search for an efficient frontier of accuracy.

But what's next for identity and the way in which marketers go about gathering related data and activating against it? Probably the most tangible new concept is that of the customer data platform (CDP). CDPs unify and organize a marketer's first-party (self-originated) customer data, which may originate with site registration data, a CRM system or another source. Those data can be used to improve and customize the customer experience in a digital environment across multiple channels, unifying the view the customer has of the brand. This is a notable inversion of the CRM construct, which seemed intent on giving the brand a single view of the consumer.

The data managed by a CDP can also be integrated into online and offline media activities. All of this should help a brand improve the lifetime value of a given customer. CDPs, while "hot" as venture capital-funded vehicles, are relatively small today but are growing rapidly. As they establish themselves more firmly, many will likely be acquired by incumbent marketing cloud platform operators, or their concepts will be more broadly adopted. This activity further raises the likelihood that CDPs will be an important lens through which marketers view consumers.

A somewhat more logistically and politically complicated approach to identity lies in the notion of the "data co-op." Marketers (and publishers who lack the scale of their competitors) can agree to pool the data they possess about their customers (where they have permission to do so) with a group of other marketers, and in so doing build out rich profiles that would not be possible without a combined effort. While we wouldn't rule out the possibility that such approaches may eventually emerge at scale, there has been relatively little traction to date on this concept.

Another relatively nascent concept in the way identity management relates to marketing comes from another acronym-fueled corner of the marketing technology world: customer identity and access management (CIAM). This group of companies, which includes the likes of Okta, Gigya (recently purchased by SAP) and Janrain (recently purchased by Akamai), makes it relatively easy for consumers to log in to a given marketer's digital properties, sometimes using a social media or other preexisting username. Doing so makes it easy for the consumer to access a marketer's content that is personalized, and that concurrently enables the marketer to monitor what matters to which consumers. While it may not scale as directly into media, it is another way in which identity-related data can help improve the lifetime value of a customer. Clearly, CIAM is an alternative to "login with Facebook," but only if the access key is not a preexisting social media identity.

With all of the data involved here — by definition, much of it either directly or indirectly capable of identifying real human beings — there are social issues to consider in the pursuit of consumer identity. This is critical in light of last year's Cambridge Analytica scandal, the introduction of

GDPR, and what will likely be increasing wariness among consumers with respect to how much of their data is made available to marketers in the future. Marketers may need to set their expectations lower in terms of how much personal information they should expect to gather about customers and prospects.

Instead, perhaps they should invest more heavily in connecting the notion of trust to their brand. Implicit in the concept of a brand is the idea that there is some trust in what a brand stands for — but historically, privacy and security is not the kind of trust that consumers automatically associate with the companies from which they buy. Brands could also make the effort to incentivize consumers to share data explicitly so there will be no surprises to consumers when their data is used.

More generally, marketers need to realize (if they don't already) that if they can't persuade consumers to share their personal data with them, they probably don't deserve it — at least not yet.

Having explored myriad ways in which marketers can gather, manage and activate data that collectively allows them to manage their customers' and prospects' identities, a more important question arises: Is all this worthwhile?

We're often reminded of the idea that a highly targeted campaign can produce high ROIs as measured by participants in the campaign (marketer, media owner and agency, among others). Add better data — such as the data that identity-based solutions might provide if none has been used before — to a campaign and ROIs would be assumed to increase as well. However, this may only have the effect of improving a tactic on a media plan, with limited success in boosting more important brand health or business metrics.

Probably the best way to use identity is to focus efforts on using data about consumers and their identities to produce insights that can impact both creative and media ideas. The data can also be used to assess many elements of campaign effectiveness in highly granular ways, and at the level of the consumer. Doing so will help marketers realize the true benefits of consumer identities.

Today, in the West and from an advertising view at least, Facebook's and Google's versions of identity are the most powerful. They may be less numerically comprehensive than Aadhaar in India (see page 28) and lacking in biometrics captured by state agencies, but they in fact know far, far more than any registration scheme. The combination of social interaction, location, transactions, preferences and implicit and explicit intent are intensely revealing. Many researchers have tested just how revealing these volunteered indicators are and have concluded in the case of Facebook that the company's data stores know more about us than our family and friends do. LinkedIn's identity graph of professionals has a unique value of its own.

Marketers  
need to realize  
(if they don't  
already) that  
if they can't  
persuade  
consumers  
to share their  
personal data  
with them, they  
probably don't  
deserve it — at  
least not yet.

# IDENTITY

---

“It is a winner-take-all game.”

This raises the defining issue of identity: how it is used and by whom. Technology historian George Dyson offers a hypothesis that data collection at this scale goes further than describing social and behavioral structures and actually creates a new reality:

“The genius — sometimes deliberate, sometimes accidental — of the enterprises now on such a steep ascent is that they have found their way through the looking-glass and emerged as something else. Their models are no longer models. The search engine is no longer a model of human knowledge, it is human knowledge. What began as a mapping of human meaning now defines human meaning, and has begun to control, rather than simply catalog or index, human thought. No one is at the controls. If enough drivers subscribe to a real-time map, traffic is controlled, with no central model except the traffic itself. The successful social network is no longer a model of the social graph, it is the social graph. Therefore, it is a winner-take-all game. Governments, with an allegiance to antiquated models and control systems, are being left behind.”

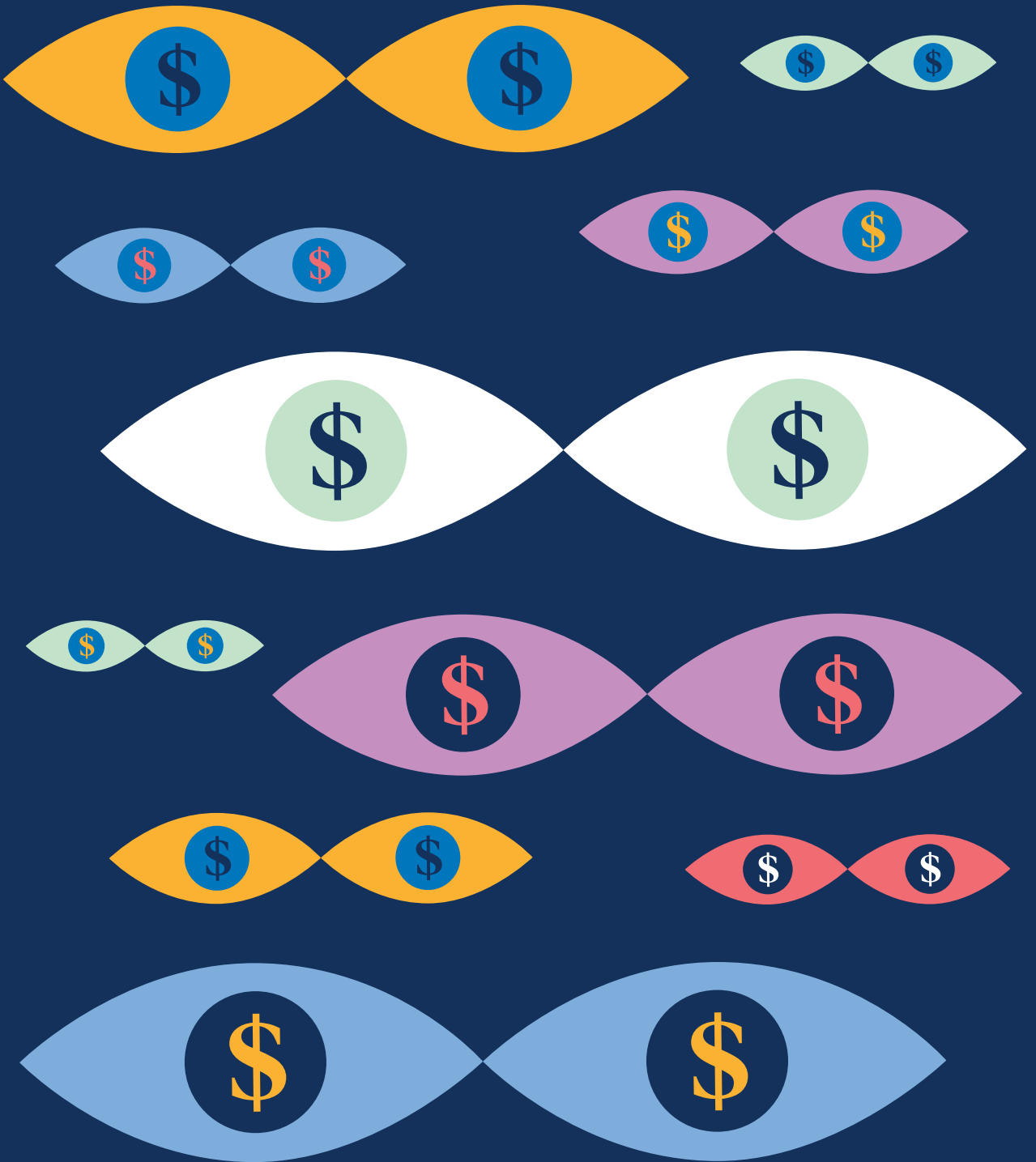
## Aadhaar — India’s great identifier

To a degree at least, the debate over acceptable use of identity is paradoxical. Populations around the world — from China by diktat, to Facebook’s “community” by choice, to every holder of a biometric passport or user of a mobile device and every Indian citizen compulsorily enrolled in Aadhaar — have sacrificed their privacy and declared their identity.

Aadhaar is especially fascinating. The Economist (2018 Christmas double issue) wrote extensively on the subject. We paraphrase parts of its work here.

Aadhaar is a 12-digit identifier issued to each of the billion-plus citizens of India. It triangulates standard identifiers like name and gender and practical ones like addresses with biometric data including fingerprints and iris scans. It represents a monumental attempt to document a society that previously combined formal social structures with no formal mechanism of identification. Originally conceived as a voluntary program to all for resource management and as a mechanism to give access to services, Aadhaar has become a necessity as many services, from health care to education and banking, are denied to the unregistered. Thus in less than a decade, a concept has created an identity graph of 1.3 billion citizens. That graph “learns” from every new “Aadhaar validated” transaction.

The comparison between Aadhaar and the giant identity enterprises of today is irresistible. The Economist describes Facebook as “the de facto identity provider of the non-Chinese internet.” One might argue the same of Google and of Amazon as they intermediate more and more interactions and transactions.



# PRIVACY

---

At its core, advertising is about influencing consumer behavior.

While some believe the point is exaggerated, it's hard to argue against the idea in some basic form that increasingly, companies view their customers as valuable data sources. That data is to be harvested in lieu of, or in addition to, payment for products and services. This thought is made more convincing by the number of businesses that opt to rely on consumer data and achieve spectacular economic outcomes by putting it to use.

The reason that consumer data is so valuable, and that companies are so keen to use it (even going so far as to risk consumer privacy), is because they can use it to capitalize on consumer preferences and more efficiently sell us their products and services. You can go a step further and argue that it's not just about capitalizing on behavior, but influencing behavior. This isn't anything new in advertising, and can be seen in just about all forms of analog advertising. At its core, advertising is about influencing consumer behavior. However, we might pause to consider how consumers feel about their personal data being used to guide their choices.

The digital identities that companies ascribe to consumers are an amalgamation of the assumptions drawn from consumer behavior online — traditionally seen as highly effective for their purposes, and part of what until now has been a reasonable value exchange. However, as we have seen over recent years in the political realm, we have perhaps been naive to its potential to fuel some unforeseen and arguably disagreeable outcomes.

A 2015 survey found 91 percent of Americans disagreed that the collection of personal information without their knowledge was a fair trade-off for a price discount, so clearly there is a tension that needs to be resolved. More recently, a Survey Monkey poll conducted for Axios showed a year-over-year 7 percent increase (to 58 percent) of the sample who believed that “the threat to privacy was now a crisis,” and a corresponding 6 percent decrease (to 38 percent) who believed that “online services were so essential as to make risk tolerable.” In the same survey, 54 percent of people said they would not pay at all to prevent tracking, and the remainder would be prepared to pay between \$1 and \$5. Perhaps this reflects the instance of actual harm perceived by the broader population?

Perhaps the answer is clearer signposting when consumer data is being used to inform what they are presented with online — although readiness to ignore terms and conditions with a simple scroll and click is well-documented. The platforms themselves might also be more explicit in communicating the value exchange. No one needs to pay for directory inquiries anymore (still available in the UK for around \$4 per minute); few pay for text messaging; video calling over Wi-Fi is free, as is photo storage; and Google Maps has saved many drivers the need to purchase navigation systems — the last of course being far less effective if it is not location aware. For all the criticism thrown at the use of data, it is hard to argue with its ability to improve the lives of consumers. Few

complain about the utility of better content personalization, relevant recommendations and (on occasion) well-targeted ads. None of this would be possible without the data trails consumers leave online.

Despite this, many consumers live in what Shoshana Zuboff describes as “The Age of Surveillance Capitalism.”

Amplifying this sentiment, Apple’s Tim Cook attacked business models relying on user data, taking specific aim at facilitating data brokers. While some may have read it as opportunistic, the idea that “consumer information is being weaponized against them with military efficiency” resonates, particularly in the wake of scandals such as Cambridge Analytica and alleged Russian involvement in the 2016 U.S. presidential election. And while it’s clear that this has been widely accepted in Europe (GDPR), the United States has not yet caught up. Although it seems inevitable that the U.S. will see some form of data privacy regulation introduced, it will likely be made more complex through a confusing and perhaps conflicting framework at the state and federal level.

The issue of privacy and exploitation of data is among the most complex of our time. Even if consumer privacy is not being unjustifiably violated, the monetization of data by major platforms has become a social, political and regulatory lightning rod.

Data security and privacy go far beyond the world of online advertising. A significant number of databases of huge enterprises have been compromised in the last two years, including email providers, loyalty schemes, retailer databases and credit rating agencies. Even more disturbing are breaches of the UK’s National Health Service, and commercial and government systems compromised by cyberterrorists, state-sponsored and otherwise. The UK Information Commissioner’s Office conducted a survey of 356 companies in 18 countries at the beginning of 2019, finding that:

- Twenty-five percent of companies had no programs in place to conduct self-assessments and/or internal audits.
- More than 50 percent of companies indicated that they have documented incident response procedures and maintain up-to-date records of all data security incidents and breaches. However, some indicated that they have no processes in place to respond appropriately in the event of a data security incident.
- Nearly 75 percent of companies appointed an individual or team to ensure compliance with relevant data protection rules and regulations.

There is a long way to go.

The issue of  
privacy and  
exploitation of  
data is among  
the most  
complex of our  
time.


# PRIVACY

## PRIVACY LEGISLATION GOING GLOBAL



Source: World Federation of Advertisers





EU – ePrivacy Regulation  
(still in drafting stage)


China – Personal Information Security Specification (May 2018)

India – Personal Data Protection Bill 2018 (expert committee issued draft; parliamentary bill expected in June 2019)


Australia – Privacy Act 1988 and amendments (last amended in March 2014, including 13 Australian Privacy Principles)

## GROUPM DATA PRIVACY BEST PRACTICE

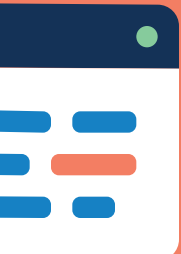
### Interrogation of Third-Party Audience & Data Vendors

- 
- What are your business objectives tied to the acquisition of third-party audiences or data? Can you lawfully use the data you intend to acquire as you plan?
  - Does the vendor have a data privacy policy, and where is it made publicly available?
  - Do you have a vendor privacy assessment checklist to enable consistent review of third parties?
  - Have you identified the consequences and remedies should a vendor fail in their answers to questions on your checklist?
  - Have you delineated employee responsibilities and authority as related to vendor review, including when they are onboarded using digital tools?
  - Does the vendor employ the same care for personal data and handling as prescribed in your own business?

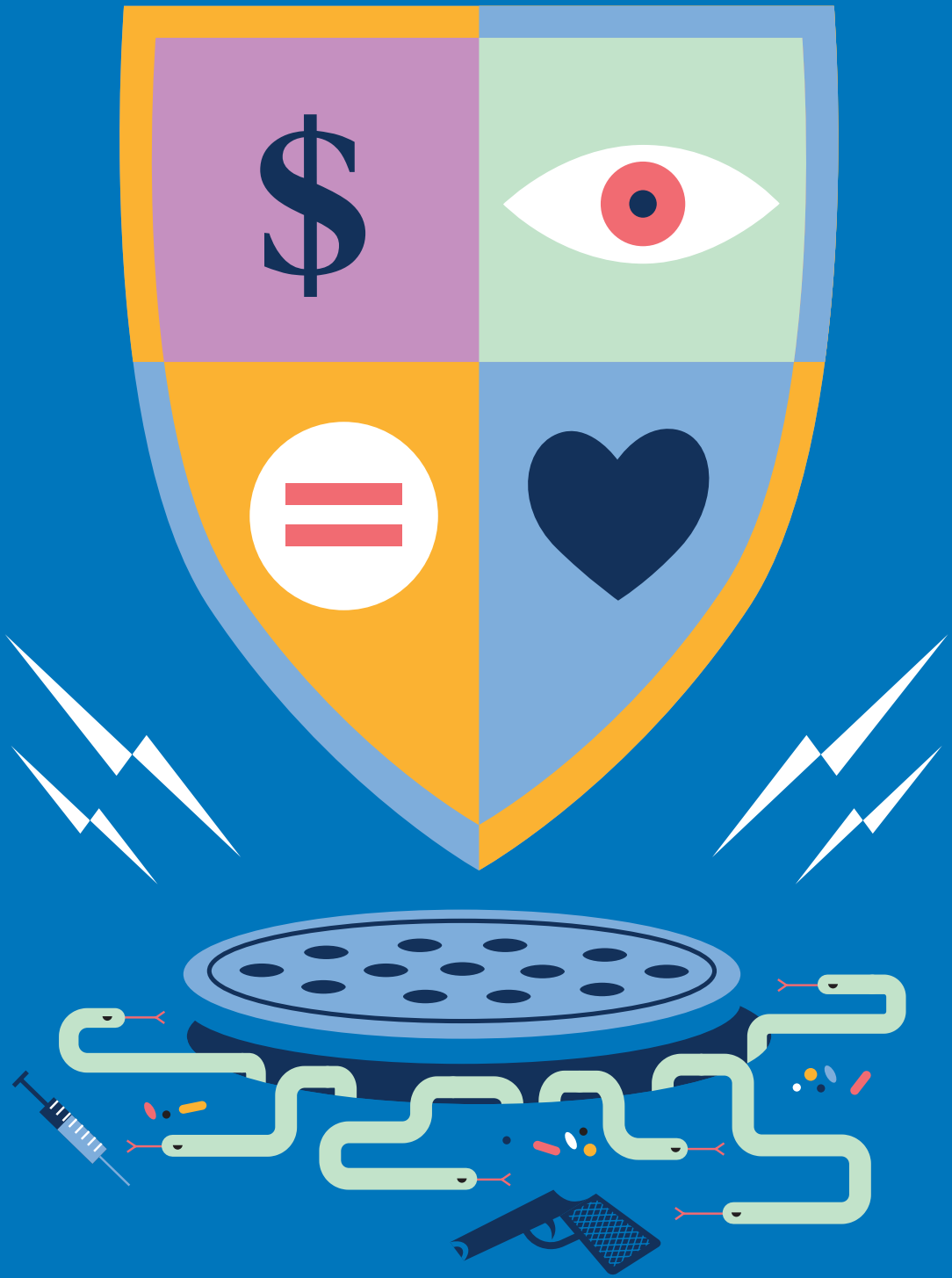
### Transparency to Consumers

- 
- Comprehensive understanding of why the planned personal data use is necessary for identified business objectives.
  - Detailed understanding of how the data will be technically processed and by whom.
  - An easily accessible display of information on why personal data is collected and how it will be used.
  - Language describing processing activities that may be understood by the average person (not educated about processing of personal data in the relevant sector).
  - A means for consumers to easily opt out of personal data processing.

### Good Tag Management

- 
- Identification of data categories for capture via tags that are consistent with the privacy notice.
  - A policy that only necessary data will be captured.
  - Clear delineation of the responsibilities held by those setting and managing tags.
  - A process for reviewing data proposed for capture via U fields to ensure alignment with the established privacy notice, or amendment of the notice as needed to support business objectives.
  - A process for notifying recipients of tag data feeds about exactly what data they should expect.

# BRAND AND SOCIAL SAFETY



# BRAND AND SOCIAL SAFETY

“Can YouTube ever be brand safe?”

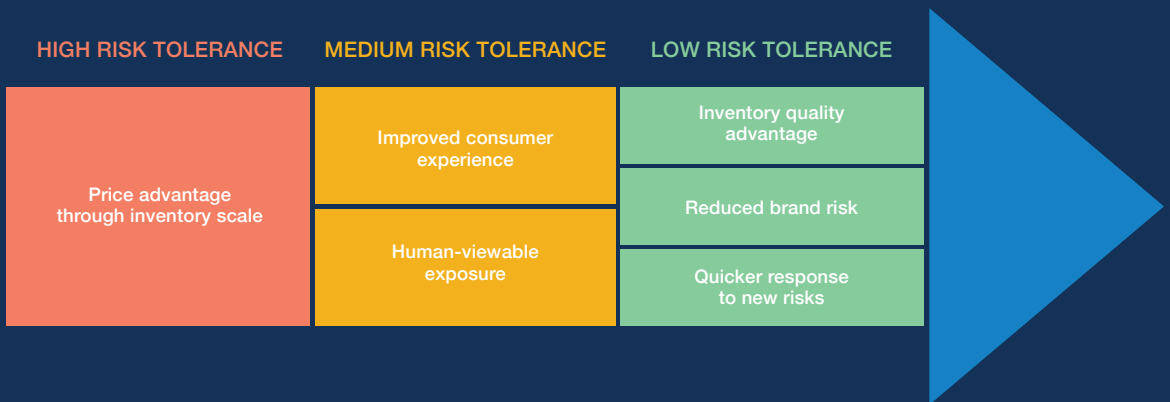
Respected technology commentator Shelly Palmer recently asked in a blog post, “Can YouTube ever be brand safe?” He concluded that if zero tolerance was the standard, the inevitable answer was no. Recently, YouTube has been criticized for allowing comments on videos of children that included time-stamp indicators of the exact moment the child was in what, to some, was considered a sexually suggestive position. Those comments have since been disabled. Similarly, the BBC carried a report in January that described the suicide of a young person whose Instagram feed suggested she was following content that explicitly described self-harm. In both cases the platforms find themselves in a tricky position and, it’s important to note, so does the public and those that see a regulatory remedy.

Commentary on brand safety is incomplete without mention of the concept of proportionality. It is true that control failures do juxtapose brands with unacceptable and sometimes vile or criminal content. The incidence of these occurrences is most likely in the category of one in several million impressions. On that basis, it is erroneous to describe the platforms as profiting from poor brand safety or to describe “advertisers as funders of terrorism.” This raises an issue for advertisers: What constitutes risk? Of course, the prominence of these incidents is amplified by the news media, and for some advertisers it is this “referred exposure” and the inference that they “fund” bad actions that they fear most. It almost always leads to negative reactions among some shareholders and customers, although there seems to be little if any evidence of economic harm to advertisers from these events.

It’s also relevant to revisit machine learning in this context. Facebook and Google deploy some of the world’s most advanced machine intelligence to classify, detect and flag unacceptable content. They do so with remarkable success, but not with complete success. A wider issue for advertisers is to assess their relationship with the sellers of media in respect to their enablement of social harm, and the reputational and economic damage that may ensue.

These “harms” include “allowing” their platforms to be used by the antisocial and the criminal — anything from live-streaming of hideous

## BRAND SAFETY RISK ASSESSMENT



# BRAND AND SOCIAL SAFETY

---

crimes, to bullying to hate speech; the promotion of illegality; and the operation of illegal marketplaces, from weapons to opioids. In some cases, whole populations have suffered awful fates because of hate being spread on platforms. There is also considerable evidence that excessive use of technology and “social” technology can have negative psychological effects on users. It’s tempting to make moral judgments, but advertisers and others should be cautious in doing so. These are rarely binary cases, and they share much in common with media that preexisted the platforms and that play a very full part in promoting extreme partiality that comes close to incitement. Fake news existed long before the internet. Even Amazon is not immune from criticism. Its sprawling marketplace business houses tenants trading in counterfeit goods and fake reviews that create social and economic harm. Hard-won reputations are easily lost.

What can we conclude from this? Open systems allow both use and abuse. When those systems also happen to be owned by the world’s richest companies, they can expect to be excoriated for anything less than perfection. If it is found that a platform knowingly allowed exploitation that caused social harm, the remedies are likely to be as punitive as any in corporate history.

Despite the issues, if the millions or billions of users (individuals, groups and businesses) of the platforms appear satisfied with the value exchange, it seems foolhardy to propose remedies that deny that value. It seems entirely reasonable, however, to expect the platforms to invest even more massive resources in continuing to enhance detection and to forego monetization of channels or groups where there is reasonable doubt as to the integrity of the content. If it means foregoing a significant portion of profits that results in depressed valuations that reflect social risks, that also seems reasonable. The platforms have legal protections in the United States that they do not have in Europe. European legislators have shown willingness to act. Further action here seems the greatest threat to the future of the platforms.

At GroupM, we are drivers of and participants in an industry-wide effort toward improving consumer experiences and protections by respecting their data-sharing wishes, avoiding ad formats that have been proven to be annoying in every part of the world, and pressuring social platforms to acknowledge their social responsibility to stop being the conduit for illegal and immoral content.

Second, we are working to better understand specific client and brand sensitivities around contextual adjacency so we can match brands with suitable content. This effort (not surprisingly referred to as Brand Suitability) requires improvement to existing semantic-based targeting and exclusion tools, moving to a more nuanced approach based on sentiment analysis and new technology in image and video recognition. This is a hard task, the complexity of which is increased if new, unintended biases are to be avoided.

As David Deutsch wrote in “The Beginning of Infinity”: “Everything that is not forbidden by laws of nature is achievable, given the right knowledge. Problems are soluble.” Let’s hope he is right.

At GroupM, we  
are drivers of  
and participants  
in an industry-  
wide effort  
toward  
improving  
consumer  
experiences and  
protections.

# DIRECT BRANDS



We are accustomed to the disruption of markets in digital goods and services. Industries as diverse as financial services, travel, entertainment, music and software have been transformed. The same is true in other sectors like retail and hospitality. A more recent phenomenon is the disruption of markets in physical goods. It has been a subject of attention by many, not least the U.S. Interactive Advertising Bureau. We are indebted to its CEO for some of what follows.

Direct brands are hard to define precisely, but share several common characteristics:

- They use a “rentable” supply chain; they tend to outsource every part of the manufacturing process to minimize fixed costs — cloud manufacturing, if you like.
- They target underserved or overpriced high-margin business segments like shaving and mattresses, which are ripe for disruption.
- They often rely on e-commerce channels — owned and operated — as well as rentable channels such as the marketplaces of Amazon, eBay and others.
- They target niche use cases that are underserved by category leaders.
- They attend to service and customer experience as much as they do to product.
- They are unencumbered by organizational silos.
- Data informs every aspect of business, from product development to demand generation and customer retention.
- They start their demand generation journey from zero-cost organic media such as search, YouTube, Facebook and Instagram and continue through to iterative testing in those channels prior to...

Prior to what? This is where it gets interesting. Almost without exception, direct brands do one of two things: They fail, like most new businesses, or they reach a threshold beyond which the strategies that got them to a certain point are no longer effective in creating new growth at an acceptable marginal cost per customer or cost per sale. At that juncture, direct brands have begun to show a new set of common characteristics:

- They move beyond the most data-enriched media to television (in the broad sense), as it uncaps potential reach of new consumers and word of mouth.

Industries as diverse as financial services, travel, entertainment, music and software have been transformed.

# DIRECT BRANDS

---

Direct brands are seen by some category leaders as an irritant and a threat, and by others as a source of inspiration and a motivating force for change.

- They add physical retail and retailer-owned e-tail to their distribution strategy to build volume and, inevitably, sacrifice margin.
- They open their own retail stores.

Thus, it's wrong to think of direct brands as either "digital" brands or as "direct to the consumer." It may be how they start, but it's rarely the way they end — if they are successful.

To date, few direct brands have arrived on the public market, and those that have tell anything but a consistent story. Furniture retailer Wayfair has delivered a fourfold return in five years, while food and ingredient delivery service Blue Apron has lost 90 percent of its value in two years. Casper (mattresses) and Warby Parker (eyewear) may well go public later in 2019. Both currently have "unicorn" status, defined as being valued more than \$1 billion by private markets.

Casper is an interesting case. It sells mattresses that are delivered direct to home. The mattresses are packed in an implausibly small box, and part of the customer experience is the "unboxing"; there is, of course, a massive unboxing meme alive and well on YouTube. The mattress category was as ripe for disruption as any because its four most notable characteristics were opaque pricing, a mostly unpleasant shopping experience, unpredictable quality, and complex delivery to the home. Casper solved for all four — like its "direct brand" peers, it followed the entire playbook as described above, did so as a first mover, and demonstrated a commitment to building a brand. Less well-known is that Casper has over 150 competitors in the "mattress in a box" category in the United States alone. The reality of direct brands is that the ability to enter stagnant markets using technology and agility means that the same strategies are as available to fast followers as they are to the first movers.

Consequently, the winners become separated from the losers by their ability to win share, retain margin, and do so on a base of awareness, familiarity and trust: in short, the identical characteristics of all successful brands.

Of course, public markets are not the only measure of the success of direct brands. Some exit to legacy players, as in the case of Dollar Shave Club to Unilever, or Bonobos (apparel) to Walmart. Direct brands are seen by some category leaders as an irritant and a threat, and by others as a source of inspiration and a motivating force for change. There is debate regarding the motivation of the buyers.



# DIRECT BRANDS

---

There are three credible arguments, one or more of which may apply in each case:

1. Direct brands can fast-track the data, marketing and e-commerce strategies of their new parents.
2. Direct brands allow larger enterprises to take relatively low penetration brands and massively scale them on preexisting production and distribution platforms.
3. Direct brand acquisitions have supplanted internal research and product development functions and moved the cost of innovation from the profit-and-loss account to the balance sheet.

These acquisitions are not without their challenges; some are operational and others are cultural. All good direct brands have committed entrepreneurs who may or may not be a fit with their new parent. One insurance against “organ rejection” has been to allow management to maintain control of branding and marketing. It remains to be seen if that succeeds over time or if the cultures can successfully coexist, especially as inevitable performance issues arise.

Direct brands are not a flash in the pan, unless there is a sudden increase in the cost of capital or a sudden increase in the agility of legacy category leaders, accompanied by a willingness to invest in self-disruption. Both are possible, but not imminent. More imminent is the degradation of data when Instagram becomes a closed-loop shopping engine as opposed to a traffic source for owned and operated commerce domains. What is true beyond doubt is that the strategies of direct brands — and in particular the role of data as an enabler of agility — have focused the minds of many legacy players in packaged goods and other categories, and at the agencies and measurement businesses on whom they have traditionally depended.

Direct brands may be the leading indicator of the future state of brand development and brand marketing.

Direct brands  
may be the  
leading  
indicator of  
the future  
state of brand  
development  
and brand  
marketing.

## A LAST WORD



## A LAST WORD

---

To those of you who got this far... thank you. It's a cliché to say that the only constant is change, but we see no deceleration in high-impact, technologically driven advances. The next decade will be dominated by advances in AI and the next wave of commercial and social disruption.

In every sector the innovation cycle will speed up, and in all fields there will be greater scrutiny of the possibility of social harm — and hopefully an equal focus on social good.

More narrowly, in advertising, scrutiny of business models that depend on the monetization of data signals will increase, as will the penalties associated with enabling bad actors. The rewards for actions that make advertising more valuable will be significant.

In the media world, existing trends will accelerate. Over-the-top delivery and consumption of video will grow, along with increased bandwidth at reducing prices. Clear winners and losers will emerge in the battle for paying subscribers. Per-user revenue strategies will vary from the flat world of Netflix to locating the 5 percent of all users responsible for 80 percent of revenue for many digital publishers. Content producers will search for the economic balance between vertically integrating monetization and the sale of content to the highest bidders. Social platforms will increasingly seek out mixed monetization models, diversifying from advertising to services and commerce.

The New York Times, with its impressive 2.3 million digital-only subscribers, counts just a little less than 2 percent of its U.S. unique visitors as digital subscribers. That's out of its approximate 100 million U.S. unique visitors, as recently measured by Comscore. ([piano.io](http://piano.io))

The role of data will continue to change, and for advertisers first-party data will be of the greatest value for understanding customers. They will use it to create audiences that will be found inside the walled gardens of the platforms, and that match with the context of publishers and the data they have on user behavior. Matching privacy and relevance will be of great importance and value.

In advertising, the “interruptive” model will persist, but delivery will be increasingly programmatic and addressable. Decisioning will be both automated and autonomous. Over time, the pursuit of mass reach via broadcast means will give way to in-target reach assembled one person, one household or one device at a time. Coupled with enough creativity and variation in messaging to address the varying needs and wants of the many customer cohorts of each and every brand, advertising has the opportunity to maximize efficiency, effectiveness and relevance. In other words, advertising will become more valuable.

[rob.norman@groupm.com](mailto:rob.norman@groupm.com); [brian.wieser@groupm.com](mailto:brian.wieser@groupm.com)

---

In other words,  
advertising will  
become more  
valuable.

# APPENDIX



## Cookies and Device IDs – The great identifiers

### The history of the cookie

In the beginning, the web had no memory. When you followed a link to a new page, everything you did on the last page was erased. There was a fresh start with every click.

It was Netscape that gave the web a memory. This happened pretty early on, when they realized there were a few issues with a forgetful version of the web. Let's say you added something to your shopping cart on an e-commerce site. As soon as you clicked to the next page to continue shopping, your shopping cart would be empty. That was a bad user experience. So Netscape built a persistent-state store — tiny, reusable, embedded bytes of code stored in the browser that let websites hand off information between page loads. That way, the shopping cart would stay full.

In computer programming, there's a word for identifying bits of information passed between machines. They're called magic cookies, named for the messages embedded in fortune cookies. Or maybe it's for the cookie trail they leave. In either case, when Netscape added a persistent-state object to their browser in 1994, they called them cookies as a tongue-in-cheek reference.

### What is a cookie?

An HTTP cookie (also called web cookie, internet cookie, browser cookie or simply cookie) is a small piece of data sent from a website and stored on the user's computer by the user's web browser while the user is browsing.

Cookies were designed to be a reliable mechanism for websites to remember stateful information (such as items added in the shopping cart in an online store) or to record the user's browsing activity (including clicking buttons, logging in or recording which pages were visited in the past). They can also be used to remember arbitrary pieces of information that the user previously entered in form fields, such as names, addresses, passwords and credit card numbers.

### Structure of a cookie

1. A cookie is a small text file that lives on your phone or computer.
2. A cookie has a name (e.g., "ID").
3. A cookie has some value (e.g., 123456789).
4. A cookie is associated with just one domain (e.g., mookie1.com).
5. A cookie will expire at some point (e.g., 13 months from right now).
6. A cookie can be "read," "set," "deleted" or "updated."

# APPENDIX

---

7. A cookie can only be read, set, deleted or updated by the website that created it.

## **First-party vs. third-party cookies (there are no second-party cookies)**

Cookies are created every time a user accesses a website. Sometimes, only a first-party cookie is created, but most of the time, both a first- and a third-party cookie are created. The difference between the two has to do with who creates them.

First-party cookies are created by the website a user visits directly. For example, if you visit CNN.com, HuffPost.com, and NYTimes.com, all those sites will create a cookie (one for each site) and save them to your computer.

Third-party cookies are created by other websites, not the website you're visiting. For example, let's say you visit CNN.com and read a few articles, CNN.com will create a first-party cookie and save it to your computer. Now, as CNN (like most other publishers) uses online ads to monetize its content, the ads you see on the pages will also create a cookie (e.g., in ads.somedsp.com domain) and save it to your computer. As these cookies are not created by CNN, they are classified as third-party cookies.

Third-party cookies are an extremely common part of online advertising, but there are a few problems associated with them. As mentioned above, one of the main issues advertisers and publishers face is the growing popularity of ad blockers and other methods that block third-party tracking.

Third-party cookies can be blocked when a user does one or more of the following:

- Browses the web in private mode.
- Uses Safari or Firefox as their web browser.
- Changes the cookie and tracking settings in Chrome or Internet Explorer.
- Uses Tor.
- Installs ad blockers or similar add-ons.

## **Similarities and differences between browsers**

All browsers, including Chrome, Firefox, Internet Explorer and Safari, have common traits regarding cookies. All browsers handle the seven cookie-structure traits listed above in the same manner. Additionally, each has a concept of first- and third-party cookies and defines them the same way. Each browser has controls about whether you want to accept first- and third-party cookies. The major differences are seen in Safari's and Firefox's default settings.

## **Firefox and Enhanced Tracking Protection**

Enhanced Tracking Protection (ETP) is a Firefox feature that provides users with the option to block cookies and storage access from third-party trackers. The change represents a shift by Mozilla from the more passive “Do Not Track” system to an active feature that blocks tracking by default and requires users themselves to opt in to a website’s trackers. Beginning in Firefox 63, users have the option to enable ETP. In Firefox 65, this option is enabled by default.

Firefox uses a Tracking Protection list to determine which resources are tracking resources. Firefox uses the built-in Tracking Protection URL classifier to determine which resources match the Tracking Protection list. Domains are matched against the list in accordance with the Safe Browsing v4 specification.

## **Safari and Intelligent Tracking Prevention**

It’s important to recognize that Safari has been disabling third-party cookies by default for a while now. More specifically, they’ve always allowed cookies to be created by a third party in a third-party context (i.e., a cookie created by a domain other than the domain of the site), but those cookies would never be persistent or accessible across sites; only cookies originally written as a first-party cookie could be accessed in third-party contexts. Consumers could override these settings, but industry data suggests this is quite rare.

Intelligent Tracking Prevention (ITP) is a Safari feature that reduces cross-site tracking by further limiting cookies and other website data. As part of its release of iOS 11 and macOS 10.13, Apple added ITP to reduce the number of tracking mechanisms that advertisers, publishers and technology companies employ. The idea was that ITP would increase consumer privacy and enhance the web browsing experience by eliminating excessive and persistent tags that can lead to slow load times. ITP puts restrictions on whether any business can continue to read or update first-party cookies when the user is not directly on the business’ site. In other words, it affects whether a company can access first-party cookies in a third-party context.

## **How does Intelligent Tracking Prevention work?**

Intelligent Tracking Prevention collects statistics on resource loads as well as user interactions such as taps, clicks and text entries. The statistics are put into buckets per top privately controlled domain or TLD+1. A machine learning model is used to classify which top privately controlled domains can track the user cross-site, based on the collected statistics. Out of the various statistics collected, three vectors have a strong signal for classification based on current tracking practices: sub-resource under number of unique domains, sub-frame under number of unique domains, and number of unique domains redirected to. All data collection and classification happens on-device.

# APPENDIX

---

There are three versions of ITP; the user's version is dependent on the version of Safari that is installed. ITP 1.1 and 2.0 build upon ITP 1.0 and further restrict access. In the latest version, ITP 2.0 immediately partitions cookies for domains determined to have tracking abilities. The previous general cookie access window of 24 hours after user interaction has been removed. Instead, authenticated embeds can get access to their first-party cookies through the Storage Access API. The API requires that the user interact with the embedded content.

ITP does not affect registered users of sites. If the user interacted with example.com in the last 30 days but not the last 24 hours, example.com gets to keep its cookies, but they will be partitioned. "Partitioned" means that third parties get unique, isolated storage per top privately controlled domain or TLD+1; for instance, account.example.com and www.example.com share the partition example.com. This ensures that users stay logged in even if they only visit a site occasionally, while restricting the use of cookies for cross-site tracking. Note that WebKit already partitions caches and HTML5 storage for all third-party domains.

In terms of overarching significance, Safari and Firefox together account for 20-30 percent of web impressions, so the impact is meaningful. If Google follows, as seems likely the same path with Chrome, the impact will be huge.

## Device IDs and identity graphs

### **A definition (just mobile or all connected devices?)**

Device graphs are used to create unified identity spaces across disparate domains. They are maps that link an individual user's record of identity to all the devices they use, which could be their computer at work, laptop at home, tablet, smartphone or even their TV. Instead of counting each device as the behavior of a different person, a device graph counts them as one person, so there's no duplication. Advertisers can then see things like what time of day a person was exposed to an ad and on which device, which helps show what role a mobile ad had in a purchase.

There are two types of graph techniques: deterministic and probabilistic. Deterministic device linkages use logged-in data, such as when a person is asked to input their email address. Facebook uses this, as does Google, along with other companies like ISPs. Probabilistic device linkages most typically use machine learning techniques to analyze behavioral and bid-stream signals that indicate multiple devices are the same person.

Most device graphs connect identifiers easily accessed and surfaced in the open ad tech ecosystem — primarily emails, desktop cookies, mobile cookies, mobile advertising identifiers and OTT device identifiers. Newly addressable devices, such as set-top boxes, and identifiers existing within walled garden ecosystems, such as Facebook and Apple, are typically not part



of a portable device graph; identity can typically be matched into those environments, but the flow of data back into the graph cannot pass back across the event horizon.

## **Their theoretical and actual value for targeting and attribution?**

The theoretical value behind device graphs is in the ability to use best-in-class point solutions for targeting and attribution, without concern for data silos and audience fragmentation. By creating a unified record of identity across every medium and access point, you can make a like-for-like assessment of the value of an impression across TV, mobile and desktop, and then act on that intelligence in the platform of your choice without sacrificing feature sophistication. Applying machine learning and automation techniques on top of a device graph-enabled data set maximizes marketing efficiencies and effectiveness.

The actual value is much more limited for two major reasons.

The first is the trade-off between scale and accuracy.

Deterministic linkages, where it is known that two identifiers represent the same person, have high accuracy but low scale across different domains. Deterministic cookie-to-cookie linkages are universally scaled, cookie-to-mobile linkages are moderately scaled, and cookie-to-PII linkages have limited scale; the industry standard for PII-based identity graphs consider a good match rate to start at 40 percent. The result, then, is that scale must be built through probabilistic matches, which frequently use black box methodologies to create those linkages, which also tend to change very quickly, with limited ability to understand how matches are made and unmade. Most important, though, is that walled garden ecosystems not only wall off inventory access, but identity access as well, which means significant parts of an advertiser's media plan cannot be sequenced or conjoined for attribution.

The second is actionability. Identity graphs are mature in how they are used from a measurement perspective, as aggregating data from multiple sources, connecting, and looking back at what happened happens outside the time demands of real-time optimization and buying. The issue is then using those outputs to adjust campaigns as they're running. Most buying platforms cannot communicate with each other, and typically operate off only one identity space, making even the simplest targeting use cases complex. Take the myth of people-based marketing: Most DSPs, even Google DV360 and the Amazon DSP, use cookies as the primary transactional and sync space. This is starting to change, however, with more buying platforms accommodating identity consortia that are incorporating universal identity providers at their base. The Trade Desk being able to transact off LiveRamp's IdentityLink, which has some of the most advanced identity graph management capabilities, is the best example.

# APPENDIX

---

## **Related regulatory issues**

Identity graphs are the greatest potential victims of more robust regulation in advertising, given the number of fronts from which they can be attacked.

Concerns around data leakage, privacy and consent exponentially multiply with every new data domain added, and a robust identity graph needs as many as possible to be useful. As a result, identity graphs need to answer difficult questions: Has a user consented to be tracked in each domain represented by the identity graph? Has a user consented to their data being shared between domains? How was the deterministic and PII-based data collected, and can it be used for matching? What signals does a probabilistic match use, does that match provider have the rights to use that data, and how can a user opt out of a probabilistic match they aren't even aware is being performed?

Every issue that regulatory hawks have with data practices in digital marketing — and the internet more broadly — is represented to some degree in the identity graph space.



**GroupM**  
3 World Trade Center  
175 Greenwich Street  
New York, NY 10007  
USA

A WPP Company



GroupM is the world's leading media investment company responsible for more than \$45B (COMvergence) in annual media investment through agencies including Mindshare, MediaCom, Wavemaker, Essence and m/SIX, as well as the outcomes-driven programmatic audience company, Xaxis. GroupM creates competitive advantage for advertisers via its worldwide organization of media experts who deliver powerful insights on consumers and media platforms, trading expertise, market-leading brand-safe media, technology solutions, addressable TV, content, sports and more. Discover more about GroupM at [www.groupm.com](http://www.groupm.com).

