CENTER FOR LONG-TERM CYBERSECURITY

CYBERSECURITY FUTURES 2020

UNIVERSITY OF CALIFORNIA, BERKELEY

The University of California, Berkeley Center for Long-Term Cybersecurity was founded to develop and shape the next generation of cybersecurity research and practice based on a long-term vision of the internet and the future of digital technology.

Cybersecurity, in our view, will encompass the key issues—those important enough to deserve the word "security"—that emerge at the intersection between technology and people. Attacking and defending today's (and tomorrow's) computers and networks is a part of that story, but only a part. In the not-so-distant future, most things (and most people) will be connected to digital networks. "Cyber" will become a baseline assumption. "Security" will also undergo a reformulation much like what happened to "national security" after the end of the Cold War, in which a term once focused on superpower nuclear deterrence grew to encompass a much broader agenda, including environmental security, economic security, and "human" security.

For these reasons we believe the cybersecurity research and policy communities will soon confront a much more diverse set of problems and opportunities than they do today. To shed light on that emerging landscape, we have developed a disciplined, imaginative approach to modeling what cybersecurity could mean in the future (which we define for purposes of this report as the year 2020).[1] Our goal is to identify emerging issues that will become more important; issues on the table today that may become less salient or critical; and new issues that researchers and decision-makers a few years from now will have wished people in the research and policy communities had noticed—and begun to act on—earlier.

To this end, we are using scenario thinking, a proven methodology for investigating expansively and purposefully how cybersecurity future(s) might unfold. Scenarios traditionally have been used by organizations to develop long-term strategies; this may be one of the first attempts to use scenarios in an academic context to help shape a policy-relevant research agenda.

In this Introduction, we review why and how we engaged in scenario thinking, the methods we employed, and the preliminary outcomes of that process.

SCENARIO THINKING AND THE FUTURE OF CYBERSECURITY: WHAT, WHY, AND HOW

Scenario thinking is a *tool for ordering arguments about alternative future environments* in which today's and tomorrow's decisions will play out. Whether used for strategic planning or identifying research priorities, scenario thinking is based on three core propositions.

1. Change and surprise in fast-moving socio-technical environments are often a consequence of unexpected and/or unexamined *permutations* among seemingly disconnected or unrelated forces of change. The world is never shaped by "just" technology, human behavior, regulation, or business models; rather, it is shaped by all of these at once, in overlapping fashion. In other words, many drivers of change work together to create new opportunities and constraints, causing new problems to arise and others to recede.
2. Some of the most important driving forces of change come from diverse domains—healthcare, markets, social norms, and the like—outside the immediate, day-to-day, tactical environment where cybersecurity experts and organizations naturally tend to focus. Analysis of these driving forces often needs to be "stretched" further than is comfortable in order to identify edge-cases where potential sources of change become most visible.
3. New, relevant, and sometimes inspirational research programs and policy concepts develop out of constructive engagement with models that incorporate these multiple dimensions of uncertainty and emphasize how the future could be different from the present in significant and discontinuous ways. In other words, scenarios are heuristic devices that highlight new hypotheses, insights, and ideas about the future.

Royal Dutch Shell pioneered the use of scenario thinking in corporate planning during the 1970s, when multiple oil shocks followed from dramatic shifts in the political, economic, social, technological, and military (among other) determinants of the global energy system. The methodology was further

developed in the 1990s by Global Business Network and was employed in a wide variety of corporate, nonprofit, and government settings. Over time, practitioners of scenario thinking determined that scenarios work best when they are treated as *hypotheses*, not predictions, and when they are used to segment, highlight, and compare some of the very different possibilities for a changed environment.

To emphasize the point: scenario thinking is *not* an attempt to predict the future or create "the" single answer to the "What will cybersecurity be in the future?" question. And it is certainly not an attempt to understand that future as a direct or linear extrapolation of current trends. Instead, scenario thinking focuses on how causes from different domains and directions intersect with one another to create discontinuities that might change what cybersecurity means. Scenarios then become a tool for investigating what needs to be understood, and what needs to be done, in order to prepare for an uncertain future as it begins to unfold and undermine assumptions that govern thinking and action today.

If we are right in our starting proposition that "cybersecurity" could mean something quite different in 2020 than it does today—both conceptually and operationally—then the value of suspending disbelief to "live in" and understand these alternative future scenario worlds becomes clear.

It is not particularly useful to debate whether one scenario is more or less likely than another—or whether these are mutually exclusive and/or comprehensively exhaustive pictures of the future. No model we know of could achieve those goals. We aim instead to provoke a discussion about what the cybersecurity research and policy communities need to do *now* in order to be better positioned for a world that might very well include some of these scenario elements.

The test of scenario thinking is not whether it predicts or portrays the future accurately. The measure of a successful set of scenarios is this: enabling people and organizations to gain insight into possible futures in which "cybersecurity" means something different than it does today, involves a broader set of actors, has meaningfully greater stakes, sits on different technological foundations, and engages core human values in a novel way.

We hope you will read and use these scenarios in that experimental spirit, and that you will share with us your reactions, questions, insights, and inspirations about both research and policy choices.

METHODOLOGY AND ASSUMPTIONS

Scenarios typically embrace qualitative perspectives and the potential for sharp discontinuities that more formal planning tools and models tend to exclude. We present these scenarios as a set of stories with causal narratives that are internally valid and logically consistent. The stories are sprinkled with indicative examples of the kinds of events and behaviors that would logically follow from the core driving forces that make up the model embedded in each scenario. These examples represent the kinds of data that would be observable indicators of a particular model but are not, again, point predictions. It is the *differences* between indicators in the five scenarios that are most important, rather than the precise examples per se.

Like any good model, scenarios also are used to generate implications. Here, those implications focus on the nature and scope of cybersecurity in each world. What cybersecurity challenges and objectives rise to the fore, and what needs to be done, by whom, in order to pursue them?

These scenarios were developed out of a process that began in May 2015. The Center for Long-Term Cybersecurity brought together a broad interdisciplinary group from universities, the private sector, nonprofits, and governments, and drew on their varied points of view and expertise to develop five prototype scenarios. Working with graduate students, the Center then elaborated on the drivers of change that were *most uncertain* and *most important* in these scenarios to refine the causal logics and illuminate their potential impacts. We tried to strike a balance between developing the richness and complexity of each narrative and making them accessible and digestible to the public as well as to professional communities. An early version of the scenarios was then made available, on a restricted basis, to key stakeholders and academics for engagement, commentary, and further refinement in late 2015 and early 2016.

Our aim in writing these five scenarios is to create a usable representation of an imaginative map of the possibility space—stretched in some respects to the boundaries of plausibility—that researchers, decision-makers, and policymakers can use to help navigate the future. As a modeling exercise, the discipline of "simplify, exaggerate the most important elements, and add the complexity back in" applies. We hope that in reading these scenarios you will seek not only to understand the core characteristics of each model that we present, but to ask yourself, "What would I need to understand and do differently if a world like this were to come into being?" Multiple answers to those questions will contribute to a forward-looking research and policy agenda that should be more robust, both intellectually and practically.

We welcome further engagement with and feedback on the scenarios via our website at cltc.berkeley.edu or via email at cltc@berkeley.edu.

ACKNOWLEDGMENTS

The Center for Long-Term Cybersecurity would like to acknowledge UC Berkeley School of Information graduate students Daniel Griffin, Elaine Sedenberg, and Richmond Wong, who wrote the first drafts of these scenarios with guidance from Professor Steve Weber, Associate Dean Jesse Goldhammer, and CLTC Executive Director Betsy Cooper; Jonathan Reiber, who provided useful consultative advice on the structure and implications of the scenarios; Faith Hutchinson and Jackie Jones, who provided stunning design assistance for this publication; Chuck Kapelke, Jenny Johnston, and Nader Namini Asl, who edited and shaped the scenarios and provided outstanding technical support; and the Hewlett Foundation, which funded this research. CLTC would also like to thank the more than 100 contributors, too many to name, who helped imagine, develop, analyze, critique, and extend the scenarios. CLTC is grateful to each and every one of them for their support.

EXECUTIVE SUMMARY

The five scenarios developed from this exercise are as follows:

SCENARIO 1: THE NEW NORMAL

Following years of mounting data breaches, internet users in 2020 now assume that their data will be stolen and their personal information broadcast. Law enforcement struggles to keep pace as larger-scale attacks continue, and small-scale cyberattacks become entirely commonplace—and more personal. Governments are hamstrung by a lack of clarity about jurisdiction in most digital-crime cases. Hackers prove adept at collaborating across geographies while law enforcement agencies do not. Individuals and institutions respond in diverse ways: a few choose to go offline; some make their data public before it can be stolen; and others fight back, using whatever tools they can to stay one step ahead of the next hack. Cyberspace in 2020 is the new Wild West, and anyone who ventures online with the expectation of protection and justice ultimately has to provide it for themselves.

SCENARIO 2: OMEGA

Data scientists of 2020 have developed profoundly powerful models capable of predicting—and manipulating—the behavior of single individuals with a high

degree of accuracy. The ability of algorithms to predict when and where a specific person will undertake particular actions is considered by some to be a signal of the last—or "omega"—algorithm, the final step in humanity's handover of power to ubiquitous technologies. For those responsible for cybersecurity, the stakes have never been higher. Individual predictive analytics generate new security vulnerabilities that outmatch existing concepts and practices of defense, focus increasingly on people rather than infrastructure, and prove capable of causing irreparable damage, financial and otherwise..

SCENARIO 3: BUBBLE 2.0

Two decades after the first dot-com bubble burst, the advertising-driven business model for major internet companies falls apart. As overvalued web companies large and small collapse, criminals and companies alike race to gain ownership of underpriced but potentially valuable data assets. It's a "war for data" under some of the worst possible circumstances: financial stress and sometimes panic, ambiguous property rights, opaque markets, and data trolls everywhere. In this world, cybersecurity and data security become inextricably intertwined. There are two key assets that criminals exploit: the datasets themselves, which become the principal targets of attack; and the humans who work on them, as the collapse of the industry leaves unemployed data scientists seeking new frontiers.

SCENARIO 4: INTENTIONAL INTERNET OF THINGS

In 2020, the Internet of Things (IoT) is a profound social force that proves powerful in addressing problems in education, the environment, health, work productivity, and personal well-being. California leads the way with its robust "smart" system for water management, and cities adopt networked sensors to manage complex social, economic, and environmental issues such as healthcare and climate change that used to seem unfixable. Not everyone is happy, though. Critics assert their rights and autonomy as "nanny technologies" take hold, and international tensions rise as countries grow wary of integrating standards and technologies. Hackers find countless new opportunities to manipulate and repurpose the vast network of devices, often in subtle and undetectable ways. Because the IoT is everywhere, cybersecurity becomes just "security" and essential to daily life.

SCENARIO 5: SENSORIUM (INTERNET OF EMOTION)

In 2020 wearable devices won't care about how many steps you take; they will care about your real-time emotional state. With devices tracking hormone levels, heart rates, facial expressions, voice tone, and more, the internet is now a vast system of "emotion readers," touching the most intimate aspects of human psychology. These technologies allow people's underlying mental, emotional, and physical states to be tracked—and manipulated. Whether for blackmail, "revenge porn," or other motives, cybercriminals and hostile governments find new ways to exploit data about emotion. The terms of cybersecurity are redefined, as managing and protecting an emotional public image and outward mindset appearance become basic social maintenance.

1. We recognize that the year 2020 is a relatively near-term horizon, and that other scenario projects could look farther into the future.

SCENARIO 1

THE NEW NORMAL

The internet of the world 2020 will evolve into something of a "Wild West," with individuals and organizations seeking protection and—sometimes—justice for themselves.

Insecurity will become the starting assumption for every online interaction—not just for experts, but for everyone. Following years of escalating headlines about data breaches, internet users will operate with the belief that, sooner rather than later, their data will be stolen and their personal information broadcast. Law enforcement will fall further behind as small and medium-scale cyberattacks become an everyday occurrence and also more personal. As the first generation of true "digital natives" comes of age (many of them having coded since they were kids), it will become normal behavior to access and interfere with other people's data. Individuals and institutions will respond in diverse ways. A few will choose to go offline; some will make their data public before it can be stolen; and others will fight back, using whatever tools they can to stay one step ahead of the next hack.

THE WORLD

This scenario portrays a world of 2020 in which most people have lost faith in institutions (private or public), technology, or anything else to protect them from nefarious actors on the internet. People will fight their own battles—either through individual efforts or by banding together as communities—in order to live their digitally moderated lives as best they can. The "New Normal" internet world may seem on first glance like "more of the same"—a continuation of the trends and technologies undercutting security in 2016. But it is actually different in kind, because the default assumption for just about everyone in this scenario (not only the well-informed or paranoid) is that essentially nothing on the internet is "safe." This scenario represents the culmination of a trend: a gradual but definitive corrosion in trust across most dimensions of what people and institutions do online that had been building for more than a decade. But the endpoint feels different—and is different—than the trend. Confidence or even hope that "anyone"—whether governments, software companies, security companies, or researchers—will be able to "fix" the problem is now gone, and the behaviors of typical internet users will change materially as a result.

This shift will not be driven by a single event or crippling digital strike from which the system could not recover.[1] Instead, the decline will be gradual and monotonic, a steady and insidious corrosion over time that heads toward a tipping point. Given the relatively limited real-life impact of security breaches when they happen one at a time, the public in 2016 tends to adjust to this evolving insecurity by quietly becoming inured to the costs of replacing credit card numbers and paying for credit monitoring services. But running beneath this apparent complacency will be an almost invisible trend heading toward a threshold effect. The end result will be that, at some point, cybersecurity incidents shift from being a "tax" or "burden" on what you do in the digital world to being the core reality of internet life. Trust will be gone.

> **. . . at some point, cybersecurity incidents shift from being a "tax" or "burden" on what you do in the digital world to being the core reality of internet life.**

The seeds of this trend have been sown over the course of decades. In 2016, security problems still are perceived as mostly happening to "other people"—small groups of individuals unfortunate enough to have their data (medical, financial, social) held by the wrong company on the wrong database at the wrong time. For most individual victims, the pain is manageable. Beyond personal angst, the main costs to the average consumer are minor nuisances, such as dealing with bureaucratic paper trails, changing passwords, or entering new credit card numbers into online accounts. While illicit hacks on major healthcare companies, retailers, and government institutions make headlines, consumers and companies do not significantly alter their communication and consumption habits.

Big hacks are already semi-regular and increasingly widespread, but the stakes keep going up. State Department communications, naked photos of public figures, and email communications detailing interoffice fights at high-profile corporations are already released into the public domain. Attacks with a social agenda

FROM THE FUTURE

http://www.cyberblog.com/feed/welcome-to-the-new-normal.htm

CYBERBLOG October 28, 2020 @ 4:40pm 905 Views

Welcome to the New Normal

+ Comment Now + Follow Comments

In hindsight, we probably should have known we would end up here.

Back in 2013, when hackers plundered credit card numbers from retailers like Target, nothing changed. In 2014, when North Korea vacuumed up 100 terabytes of digital dirt from Sony Entertainment, nothing changed. In 2015, the Chinese government snatched nearly 21 million records of Americans who had worked or applied to work for the US government, but nothing changed. Even in 2018, after hackers affiliated with ISIS exposed two years' worth of Google Drive data on 50 million users—including high-ranking government officials in the US and Europe—politicians lit up the talk shows with chatter, but in the end, nothing changed.

Any of these events might have sparked a massive global call to action. Instead, the slow drip of crime corroding our online security has kept on dripping, and internet users around the world have become inured to the data breaches and headaches that go along with them.

The period between February 2019 and February 2020 saw more than 2.1 million reported cyber incidents, roughly 1.3 million more than the year before. As the first generation of true "digital natives" has come of age, there are more hackers than ever—and fewer resources to fend them off. Stealing data has become the 21st-century equivalent of toilet-papering a house. Last month alone, a group of teenagers in Iowa City shut down their high school's virtual classroom to get out of a final exam; a woman in Maine remotely drove her cheating husband's car into a lake; and fans in Pakistan rerouted a private live-stream and ensnared a top Australian cricket player in a doping scandal.

Ironically, the US government may have itself to blame for the staggering number of cyberattacks, as Congress caved in to the FBI and intelligence community by supporting weak cryptography standards and enabling "backdoor" access into the largest communications networks. At the same time, advances in high-performance computing, known exploitable biases in existing encryption standards, and vulnerabilities introduced by user error have weakened faith in encryption as a workable and effective security solution.

For the millions annually victimized by small-time cybercrimes, justice has been hard to come by. If you don't operate a hydroelectric power plant or fall prey to an attack meant to shut down the stock market, your grievances are unlikely to garner much attention or resources. Your ex-girlfriend doxed you? Nobody but you really cares. Nosey neighbor sniffing your packet traffic? Too bad. Your two-factor authentication was hacked and money or data stolen? Your fault for not moving to multifactor authentication. Welcome to the year 2020. What will 2021 bring?

(think Ashley Madison) have already become more common. While publicly decrying these actions in social settings, many internet users secretly hunt for these images and details online. It has all been very shocking, but at the same time appealingly voyeuristic, like a new style of reality show. All of this is unfortunate and annoying, but not transformative. The mindset of most consumers remains steady: "Really bad things could happen on the internet to anyone, but they probably won't happen to me."

While illicit hacks make headlines . . . consumers and companies do not significantly alter their communication and consumption habits.

This scenario imagines the next frontier in data insecurity, in which growing vulnerabilities in a wide array of internet features—for instance, the well-publicized September 2015 attack on X-code affecting the Apple app store [2]—force broader swaths of internet users to realize that nothing online is safe. Security experts have known this for years, but their efforts to explain it mostly fell flat, much like the early explanations of climate change risk in the 1990s. In this scenario, their warnings can no longer be denied.

By 2020, widespread data breaches will affect nearly everyone who does anything meaningful online, thanks in part to the rapid expansion of illicit markets for stolen information. Already teeming with activity designed to exploit personal information, this deviant industry will grow quickly as increasingly professionalized profiteers put pressure on hackers to produce and sell data at a faster rate. Their methods and tools will make electronic systems more vulnerable and the technology and expertise needed to exploit digital systems cheaper and easier to obtain. Growth in the information black market will spill over into a premium market of "hackers-for-hire," in which specialists can be hired to facilitate large-scale hacks at a steep price. Local "digital mafias" will emerge first in online communities and later in cities across the world, where they will be capable of carrying out hybrid physical/cyberattacks.

This trend will lead to an accelerating growth cycle in criminal and illicit data, an innovation cycle much like those that occur in the licit world, with the same characteristics of positive feedback and increasing momentum. In 2011, Marc Andreessen captured this dynamic when he said that "software is eating the world."[3] In 2020, he might say that internet crime is doing the same.

With internet crime almost normalized, the knowledge and programs needed to pull off digital attacks will quickly proliferate. It will become normal for individuals and digital mafias to carry out acts of revenge through hacking. "Digital natives" who grew up online will prove particularly adept and creative at pulling off these crimes. The kind of cyberbullying through social media that people worried about in 2016 will give way to personal, small-scale petty cybercrimes that—whether motivated by revenge, curiosity, frustration, or boredom—will pile financial and sometimes physical damage on top of embarrassment and harassment. Tomorrow's cyberbully won't just spread nasty rumors about your child on Facebook. She will brick his phone, lock your garage door in the "open" position, and flick the lights

on and off in your bedroom all night long. And you won't have much recourse available, other than to get in line for help from . . . who exactly? Local police? ISP technical support? Cybersecurity firms that are mostly focused on defending large enterprises? Or perhaps your "friendly" digital mafia team that can strike back in small-scale acts of "active defense"?

With internet crime almost normalized, the knowledge and programs needed to pull off digital attacks will quickly proliferate.

At some point, the political narrative will likely shift (much as it has for some in the United States around gun violence) to "it doesn't have to be this way. We just need to agree on commonsense actions to change it." But (again, as with gun violence) there will be no consensus to act decisively, and the lack of investment in law enforcement and security infrastructures will belie the rhetoric. In some cases, under-resourced police forces, already struggling to make progress or stay even with the advance of major internet crime, will give up responsibility for the digital sphere because of the growing number of small attacks and the widely distributed damage to individuals and property. This dynamic might also become self-reinforcing:

- Many criminal hackers will evade detection by keeping their impact just under the media's radar and by exploiting weaknesses in cross-jurisdictional coordination. Small, distributed internet crimes will prove more foolproof and more profitable than traditional petty theft. Talented criminals will be able to walk this line most effectively, while less talented and sloppier criminals may find themselves pushed out into other kinds of crime or employed as relatively low-wage workers in the illicit money machines run by more successful thieves.
- Decision-makers will find it difficult to appropriate increased funding toward combating these crimes in an austere economic climate where individuals and families are losing assets and where the efficacy of countermeasures remains uncertain. State and local governments will feel increased pressure to shoulder the responsibility for place-based hacking, even though true locality will often be difficult to identify. At the same time, local and regional law enforcement agencies will struggle to staff a technically savvy workforce due to the low wages they offer, the monotony of investigating small-scale hacks/stalking/vandalism, and the inability to properly investigate and bring suspects to justice, particularly as digital jurisdictions do not follow traditional geographies.
- Private-sector firms that depend heavily on e-commerce will call for solutions as they witness the detrimental impact of rising internet crime on their markets and business plans. A coalition of the biggest players might, in theory, join forces to help people around the world combat digital insecurity, but that nascent coalition will be hamstrung by anti-trust law, competitive dynamics, and

the companies' own (ironic) complicity in the problem (having waited too long to do enough about it). Meanwhile, cybersecurity firms and their venture capital backers will be focused principally on enterprise security, not the security of families, individuals, and their connected homes. As a result of these pressures, digital firms will protect themselves first and foremost, allowing the public to bear the brunt of the losses. Firms that cannot afford such protections will be pushed out of the market and, as a result, online innovation will slow incrementally but noticeably. Minimal security and minimal trust will become the new barriers to entry for startup firms.

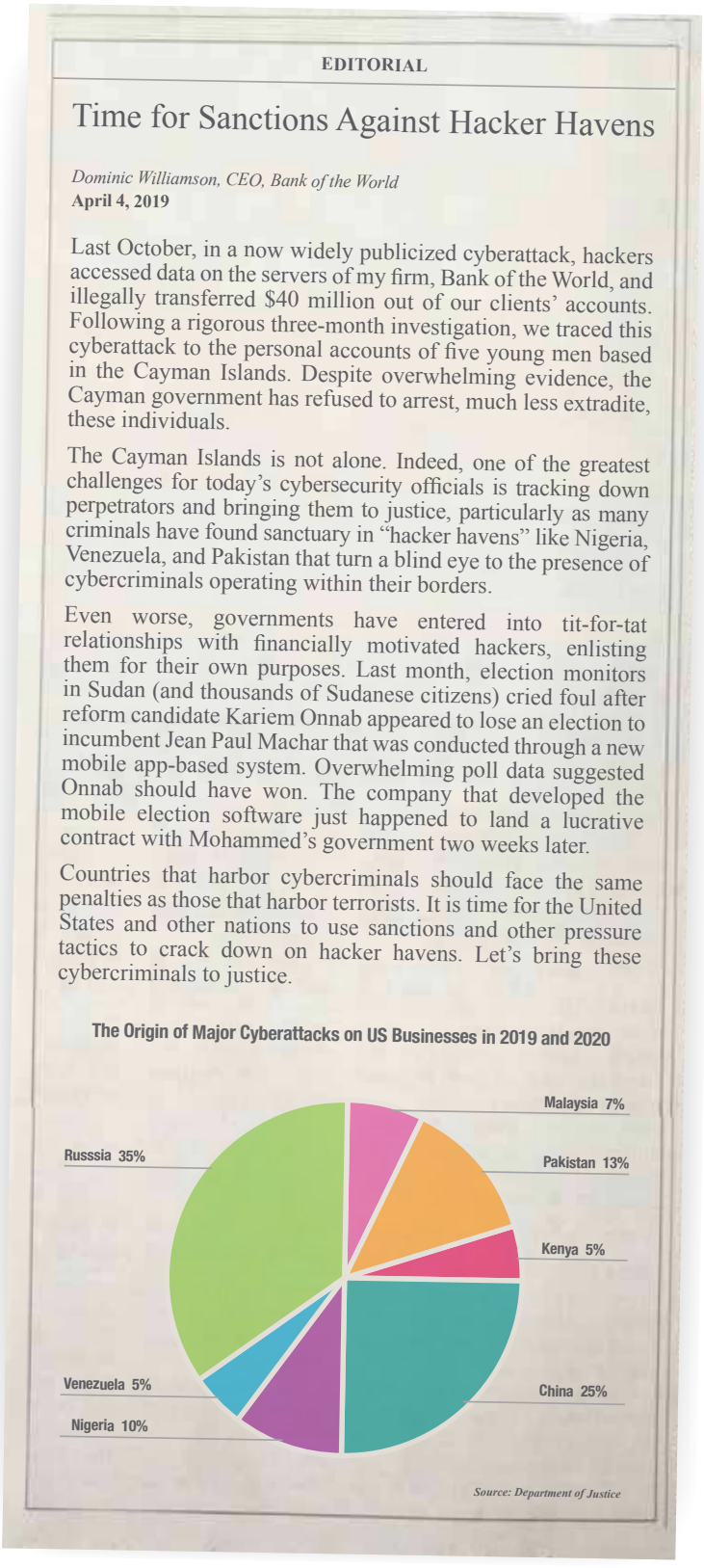
This slow-moving tsunami of small and medium-size criminal enterprises[4] will be hard to stop or even slow down. In the United States, continued Congressional polarization, along with diffuse and multijurisdictional responsibility for cybercrimes, will result in more of the same: an ongoing lack of appropriate laws to prosecute small-scale internet crimes. Prosecutors will be hamstrung by limited and outdated statutes (like the Computer Fraud and Abuse Act [5]) that restrict prosecutions to serious financial crimes. The global footprint of the hacking mafias will further complicate law enforcement's response. Because successful prosecutions require multinational cooperation, the United States will become highly dependent on international support to succeed in law enforcement—as will other countries.

Hackers will seek sanctuary (either physically or virtually) in precisely those states that refuse to cooperate with international law enforcement. These so-called "hacker havens" will benefit from the presence of illicit criminal enterprises, which bring wealth and prosperity to previously destitute and remote areas. Authorities will use diverse tactics—such as offers of fake job interviews to lure suspects into the United States,[6] or waiting until suspects move to locations where law enforcement is more cooperative—but these ultimately will have little measurable impact. In extreme cases, hacker havens could become profitable enough to drive significant economic development in some countries—a kind of deviant version of Information and Communication Technologies for Development (ICT4D)[7] —leading those governments to offer more than passive protection.

Internet users will prove stunningly resistant to altering their online behaviors, despite the escalating risks.

Can the encryption-security infrastructure reverse these trends? Human behavior more than anything else makes that unlikely. Internet users will prove stunningly resistant to altering their online behaviors, despite the escalating risks. Encryption systems will provide a significant measure of information security, but their adoption will remain limited due to lack of usability and failed implementation of best practices. The average internet user, unwilling to fully encrypt his/her web activity, will make the situation worse through the simplest mistakes: writing down passwords, leaving computers unlocked, or simply forgetting to encrypt. Once hackers improve their ability to access password aggregator websites (which will be seen as a top target), the obstacles to serious password protection will only heighten. The development of biometric or other physical passcodes will work

FROM THE FUTURE



EDITORIAL

Time for Sanctions Against Hacker Havens

Dominic Williamson, CEO, Bank of the World
April 4, 2019

Last October, in a now widely publicized cyberattack, hackers accessed data on the servers of my firm, Bank of the World, and illegally transferred $40 million out of our clients' accounts. Following a rigorous three-month investigation, we traced this cyberattack to the personal accounts of five young men based in the Cayman Islands. Despite overwhelming evidence, the Cayman government has refused to arrest, much less extradite, these individuals.

The Cayman Islands is not alone. Indeed, one of the greatest challenges for today's cybersecurity officials is tracking down perpetrators and bringing them to justice, particularly as many criminals have found sanctuary in "hacker havens" like Nigeria, Venezuela, and Pakistan that turn a blind eye to the presence of cybercriminals operating within their borders.

Even worse, governments have entered into tit-for-tat relationships with financially motivated hackers, enlisting them for their own purposes. Last month, election monitors in Sudan (and thousands of Sudanese citizens) cried foul after reform candidate Kariem Onnab appeared to lose an election to incumbent Jean Paul Machar that was conducted through a new mobile app-based system. Overwhelming poll data suggested Onnab should have won. The company that developed the mobile election software just happened to land a lucrative contract with Mohammed's government two weeks later.

Countries that harbor cybercriminals should face the same penalties as those that harbor terrorists. It is time for the United States and other nations to use sanctions and other pressure tactics to crack down on hacker havens. Let's bring these cybercriminals to justice.

The Origin of Major Cyberattacks on US Businesses in 2019 and 2020

Source: Department of Justice

well as a short-term fix—until that data gets hacked too, at even higher cost to the victims.

Some countries may mandate controversial backdoors in crypto standards[8], setting up a modern-day security dilemma[9] or "spiral of insecurity": such backdoors will not only make encryption systems vulnerable, but will increase incentives for criminals to pursue additional entries. There will also be pressure to restrict the export of encryption technologies and even make some encryption illegal.[10] The expert community will be nearly unanimous in its opposition to these measures, and for very good reason. But terrorists' inevitable use of encrypted communications—accurately reported or otherwise—will compel governments in many parts of the world to head in a different direction. Meanwhile, advances in high-performance computing may favor "crackability" over encryption security—or, at a minimum, will set off an even more vigorous race between encryption and the ability to break it, including in the realm of quantum processing.[11]

This is how we end up at "The New Normal": growing concerns about personal safety + significant and lucrative success by hackers + perceptions that internet industries are imposing upon society the risks and burdens of security failures = an increasing degree of "heads I lose, tails you win" sentiment among normal internet users. As trust in the system collapses, the baseline reality of the internet will change such that everything is insecure. By 2020, the internet will feel like an extremely dangerous neighborhood where you tread at your own risk, and where everyone is pretty much on his or her own.

OUTCOMES

"The New Normal" may seem in some respects like a straight-line extension of 2016, at least in terms of its causes and driving forces. But once people and institutions cross the perceptual threshold from security to insecurity, how they make decisions about their digital presence will change significantly. In a world where almost everyone starts from the presumption that "digital" means "insecure" and all internet-enabled devices (including billions of newly connected "things") are hackable, the security landscape will shift its focus away from preventative efforts to reduce vulnerabilities toward mitigating the consequences of pervasive insecurity through threat and attack response.

Individuals and institutions will face a new menu of possible actions and choices. Three will predominate. Important data and transactions will be: (1) "protected" through legal means that limit the use of data (e.g., medical records need not be private because discrimination or adverse uses will be illegal); or (2) shifted offline, in an attempt to manage insecurity (e.g., mobile banking will be limited and in-person transactions will be encouraged to minimize risk); or (3) performed with an assumed base level of risk that data transacted digitally will not be confidential.

How individuals adapt to this environment of ambient insecurity will be quite granular and complex. But over time, the general population will likely segment into three broad groups: those who embrace transparency as a way to undercut the value of stolen data (the "open sourcers"); those who resist the culture of openness and boost their privacy through various arcane practices ("the resisters"); and those who detach from digital networks (the "neo-luddite rejectionists" or "neo-Amish").

Some neo-luddites could adopt a more extreme isolationist approach and move to rural communities that largely reject the use of post-1970 digital technology

"Open sourcers" will embrace the electronic world's inherent vulnerability by making their data transparent by default.[12] Their logic will be simple and extreme: information cannot be stolen, manipulated, or held hostage if a definitive version has already been made public. Some people will go so far as to release read-only versions of their hard drives and email histories on new websites ("TakeMyData.com" or the like), essentially giving up confidentiality in order to reinforce their confidence in the integrity and availability of their data.

Transparency has limits, of course, and everyone has sensitive secrets that he or she tries to keep behind tightly guarded doors. But overall these individuals will manage their vulnerability by hiding "in plain sight". This kind of radical transparency will have some strange manifestations, like people posting nude pictures of themselves to fight the stigma faced by women who have been exposed or "doxed", or a new kind of campaign to voluntarily publish tax returns, bank statements, and other financial data. Norms about what is public and private change, and some will find this radical transparency empowering, seeing it as a way to make ambient insecurity their choice rather than a condition imposed upon them by criminals and technology.

"Resisters"—individuals who resist and try to hold on to higher levels of privacy—will face constant, unrelenting pressure to deploy new practices and technologies (such as bots and GPS spoofers) to protect their data and actively obscure their actions. These efforts will take far more time and effort than they did in 2016 and will only sometimes prove effective. But some techniques will succeed in controlling the illicit flow of personal data streams. There will be widespread fear-mongering, and snake-oil salespeople will target this group, offering the "next great security tool" or do-it-

yourself measures to stave off potential hackers. It will take a great deal of time, money, and expertise to avoid being duped into a false sense of security. Some individuals in this group will find ways to self-select into their own restricted-access communities that disallow any outside (or only NSA-certified or equivalent) technology to enter their gated walls.

"Neo-luddite rejectionists" (though they would almost certainly reject this label as being pejorative and anachronistic) might be young reactionaries seeking a temporary respite from modern digital experiences, or very rich people for whom digital conveniences are no longer worth the price. They also might be families with traditional values who embrace a life largely disconnected from digital networks. And they might appear in surprising parts of the world—including among vibrant technology clusters, where the costs of insecurity are best understood.

Within this group, "dumb" phones and "disconnected" homes will make a resurgence, and some people will make their best effort to eschew the use of cellular devices and sensors altogether. Given the proliferation of sensors around large population centers, some neo-luddites could adopt a more extreme isolationist approach and move to rural communities that largely reject the use of post-1970 digital technology. They may be less likely to appear in developing countries, where national infrastructures of 2020 may not allow such wholesale disconnection. It is difficult to reject technology if you require internet access to obtain your monthly water ration, for example.

Of course, few people will fit neatly into one of these ideal-type categories. Rather, as individuals come to grips with the new realities of digital insecurity, they will decide which aspects of their lives to allocate to which response pattern, and they will respond in nuanced and highly contextualized ways. Inevitable and difficult-to-manage frictions will emerge at the interfaces and edges, both between people and communities and within individuals managing different aspects of their lives. Imagine applying for a mortgage loan when banks require that your tax returns have been public for at least three years—2020's version of "proof" (to both the public and shareholders) that you are a secure investment.

INSTITUTIONAL REACTIONS

Companies, industries, local and national governments, and global crime syndicates will also start adapting to the new baseline assumption of insecurity, not security, leading to some profound changes as a result. For example, the full recognition of deep digital insecurity will impact the structure of cities and "communities" of all kinds. Many physical communities will create specialized local networks, such as "cyber neighborhood watches," in order to protect themselves. These communities will try to make secure information and communication exchange possible within limited geographic areas, particularly neighborhoods, while also trying to separate (to the extent possible) from the broader internet. On a small scale, "gated" communities may take on new meaning, with visitors required to leave unverified devices at a physical or perhaps digital security booth. Larger cities will probably see better success in banding smaller communities and neighborhoods together to minimize exposure to "outsiders," providing more herd-like protection through interlocking community watchdog organizations.

Communities with high levels of social capital will have to turn some of that capital toward developing digital public goods. That might take the form of a new wave of online "broken window policing" or the emergence of a cyber equivalent of New York's 1990s mayor Rudolph Giuliani, with zero-tolerance policies for bad behaviors.[13] But few communities will find enough social capital to make these policies stick. "Surfing Alone" will become

FROM THE FUTURE

Neighborhood Digital Watch

2/29/2020

Happy Leap Day! Join us next Wednesday, March 4, for an important meeting about keeping our neighborhood's network secure. Use your private key to access our group's Cisco Secure Connect Meeting Room, and contact our administrator, 1419&kT501$214, through TorMessage to receive your personal access key.

8 Prevention Tips and Reminders

Together we must be alert and observant in order to stop rampant trespassing, petty theft, vandalism, stalking, bullying, voyeurism, and sabotage. Here are some tips for preventing and coping with local network crime.

1. CCR: Clean, Change, and Review: Clean up old accounts, change outdated passwords, and review security software updates for your household connected devices. Abandoned devices create vulnerabilities for our localized network!

2. Keep your digital presence tidy. Overgrown file spaces create places for malware and network intruders to hide.

3. Talk to your neighbors about their security practices. Do they have biometric or multifactor authentication in place? Ask us for free e-brochures!

4. Watch out for suspicious activity coming from one another. If it looks like a bot or intruder, report it to the appointed local network administrator and file a formal complaint with the regional digital police.

5. Spot a Bot! Community prizes will be given to those who spot intruders on our neighborhood accounts, services, and networks!

6. Local businesses are our neighbors, too. Watch out for signs of vandalism on their sites and online postings.

7. Protect yourself and your family. Host an identity and personal data collection seminar in your home to learn along with your neighbors.

8. Join a cleanup taskforce to help periodically tidy up and patch our neighborhood network. Even when we are vigilant, our networks will still be vulnerable to attacks.

Recent Incidents

2/21/20: Domestic Incident. Operating from another state, a man used his ex-wife's breached Fitbit data to announce her re-entry into the dating world and local nightlife scene. He threatened to release more of her data but his packet-sniffing was detected by her digital bodyguard and his point of access into her home network was discovered and secured.

2/25/20: Vandalism. A local restaurant, Fork, had its web presence defaced with claims that the company served "roadkill" and other vile offerings. This incident resembled the attack on Spoon on 1/10/20. During the community cleanup of the website, a volunteer noticed a digital signature that led us to local restaurant, Knife, as the vandal. A local boycott of Knife is now in place. Mention this notice and receive 10% off all cash purchases at Fork.

2/25/20: Stalking. An unknown assailant followed a teenage girl home from school over the course of a week. Our Neighborhood Watch helped her use a GPS-spoofer to send her unknown stalker into a trap. No charges were filed, but the neighborhood has identified this man and attached his picture to the back of this flyer. Stay alert!

the latter-day equivalent of "Bowling Alone"—an activity that signals a lack of social capital and a deterioration in community cohesion, safety, and joint action.[14]

Commerce will, of course, be deeply impacted by the changing norms of internet activity. If the starting assumption for customers becomes internet insecurity, some industries—notably, but not limited to, banking—will retreat to delivering primarily offline services to consumers. In a dramatic reversal, offline transactions will once again become the default. The reversion to paper and in-person communications will make physical co-location increasingly important. Tremendous advantage will accrue to current financial centers (New York, London) and tech centers (Silicon Valley, Tokyo) that already have co-located companies and employees.

In sectors where online transactions are less sensitive, there may be a resurgence of non-neutral intermediation platforms (like the early AOL) that provide a proprietary security layer for sensitive online operations like logins and purchases. These platform companies (Google and Apple, perhaps?) would receive more of users' data in exchange for providing better security than most could achieve on their own. However, because such platforms would not be foolproof—indeed, they would be high-value criminal targets—their use might be limited. Top companies would also come under regular anti-trust scrutiny, given the regular cross-corporate cooperation on security vulnerabilities and the added power that companies have over consumers.

Some industries, like healthcare, will benefit from this environment of insecurity in surprising ways. In the United States, laws that were designed to help keep information private, like the Health Insurance Portability and Accountability Act (HIPAA), will create significant and sometimes insurmountable transaction costs for the sharing of health-related information in research and clinical settings. Moreover, in this scenario HIPAA will become nearly irrelevant, because many patients will voluntarily make information more available, enabling healthcare providers to access and process health-relevant data with much greater ease. We might see a rapid increase in new insights and therapies that have a self-reinforcing impact on the willingness of patients to make their previously private data (available to criminals but not to legitimate healthcare providers and researchers) public.

HIPAA will become nearly irrelevant, because many patients will voluntarily make information more available.

Of course, some individuals will hesitate—even more than they do today—to have certain illnesses treated (psychiatric problems, for instance, or degenerative mental and physical conditions) out of fear of having their health records made public and feeling the associated stigma. But the opposite could also happen: norms sometimes change quickly when information about previously "secret" conditions can't be kept secret anymore. Consider mental illness. Thomas Eagleton, the US Democratic Party's 1972 vice-presidential candidate, had to withdraw from the race when information about his history of depression was leaked to the press.[15] Twenty years later, President Bill Clinton talked openly about his psychotherapy, as do many people in public life today. If most or even all medical records were in the public domain, how many conditions would remain stigmatized for long—particularly if there were laws that effectively constrained discrimination on the

FROM THE FUTURE

STRANGE AS IT SEEMS, "LEGACY" COMPUTER SYSTEMS ARE ALL THE RAGE IN GOVERNMENT SECURITY.

Washington Tribune
July 15, 2019

NAIROBI – A group of government and business leaders from across Kenya gathered in the capital on Wednesday to consider their next steps following a massive cyberattack on the nation's new mobile banking platform. The attack left 20 million without access to funds for a three-week period.

The source of the attack is uncertain, but rumors suggest it may have been launched by Kandaya, a growing social group seeking to pressure the government into passing more conservative laws. Others have pointed to international criminal syndicates.

One of the key questions the government leaders will ask: how did the attack happen, given that the Bank of Kenya recently plunged 22 billion Kenyan shillings ($220 million USD) into a new software system specifically designed to offer state-of-the-art security?

"We just spent a huge amount of money, and we are less secure than we were before," says Michael Mburu, leader of Digital Kenya Network, an activist organization. "Someone has to be held to account for this."

Kenya is one of many countries that have felt pangs of buyers' remorse in recent years, and it turns out they may have good reason. A recent United Nations report found that the more obsolete and decentralized a nation's computer network is, the less susceptible it is to a large-scale cyberattack.

"'Heterogeneity' is the new buzz word," says Amelia Wright, an analyst with Digitati Solutions, a Washington-based cybersecurity contractor that helps governments around the world protect critical infrastructure. "In the past, having a mix of systems and software was seen as a disadvantage for interoperability and efficiency. Now, integration is a recognized source of vulnerability."

The recent hack could have a significant impact on digital systems procurement in the United States. The military and other government agencies have been pressured for years to update "legacy systems," but now are recognizing that these old systems—many of which are based on COBOL and other coding languages that have largely fallen out of favor—are in fact an advantage.

"The US was one of the first countries in the world to build out its computer networks, in many cases long before the internet was invented, and now that turns out to be a major security advantage," Wright says. "Sadly, developing countries that were not saddled with legacy systems have bought into modern, integrated systems that are the most vulnerable to hacking."

basis of that knowledge, as laws do today around visible disabilities?

Similar dynamics might unfold in education. If data about students were by default public, school districts would have to become more adept at leveraging that data to improve teaching. At the same time, governments would have to step up quickly and boldly to constrain illegitimate, discriminatory, and undesirable uses of such data. Decisions that are now often made quietly and indirectly, such as segmentation of students by ability, would have to be debated openly. Long-known but unspoken biases (for example, in admissions processes at selective colleges) would

become transparent to outsiders. Once these data sources are no longer privileged and private, how long could institutions like these argue that their algorithms for processing and drawing insights from data should be held secret?

For governments, "The New Normal" could be a very different world in terms of public-sector actions and responsibilities. At the highest level, cybersecurity will no longer be treated as a baseline public good for which the state is ultimately responsible (even if that belief was mostly illusory in 2016). Rather, it will become—in perception and reality—more like a narrow service provided by defense departments and other specialized government institutions to support a limited number of critical public safety objectives, a form of critical infrastructure.

Within the United States, government agencies will experience important shifts in power. Intelligence agencies may benefit at first from the availability of vast new open data sources, as messy, noisy, unstructured, and likely biased as they might be. But they will also face a decline in their traditional sources of leverage, as former "secrets" will be increasingly made public. As a result, these agencies will move into new domains of practice. The NSA might take on an expanded set of intermediary roles—for example, certifying the validity and reliability of certain security fixes in exchange for participants agreeing to have their data screened by NSA systems (akin to an Underwriters Laboratories for security[16]). Other domestic government agencies will struggle to keep up with the flow of data, and the public will get out ahead of what those agencies would be ready to release through "open government initiatives." This will be particularly challenging when agencies are required by statute to protect data that is suddenly, as a result of private individual action, in the public realm.

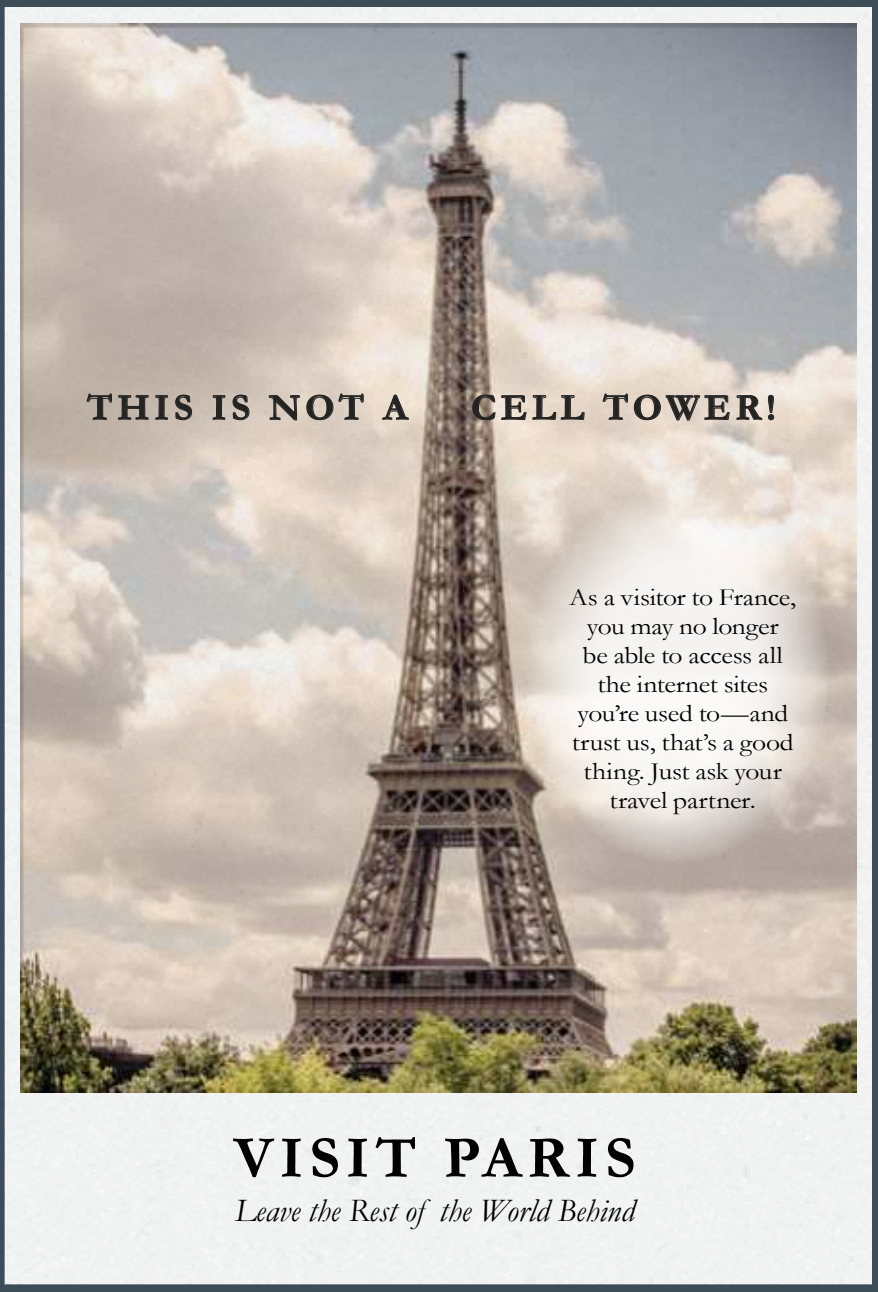
Governments will reshape the most significant forces of demand facing the cyberdefense industrial complex. Instead of asking contractors to build systems that protect huge, widespread systems and assets, the challenge will be to offer extreme protection to a relatively small number of assets, which in turn will be under more intense scrutiny and higher risk of attack. Almost every battle will become high stakes, and every failure a potentially catastrophic loss.

For governments, "The New Normal" could be a very different world in terms of public-sector actions and responsibilities.

At the same time, increased transparency, combined with increased cybermilitary capacity, will render "digital wars" and "cyber Pearl Harbors" even less credible. Of course, countries that invest heavily in strategic cyberattack capabilities will not give them up altogether. Instead, they will modify their strategic focus, doubling down on the capacity to carry out very large attacks that truly put other states at deep risk. Because the ability to carry out small and medium-size attacks that create moderate levels of "cyberinsecurity" no longer has any meaningful impact, states will instead focus even more strongly on preparing for big attacks on major and vulnerable systems. This will add to tension in the Sino-American cyber landscape in particular and also give rise to a dynamic much like a bipolar nuclear balance of terror. Somewhat ironically, it might also yield a higher level of strategic stability, at least when it comes to state-to-state cyberwar worries.

FROM THE FUTURE

European countries are experiencing a significant shift in their views about online access and privacy. Estonia, which in 2018 passed some of the world's strongest cybersecurity legislation, has since seen a marked decrease in cybercrime. Estonia's approach, which includes limiting access and imposing greater central controls on internet activity, is now being considered a model by other EU nations. France, for example, is currently debating a proposal that would strictly limit internet access, particularly for foreign visitors. The French Tourism Bureau has already mocked up a campaign that would tout the country as a "romantic and vintage" destination where the lack of online distraction is a benefit.



State-based distinctions in cybersecurity regimes will become tauter and cause additional friction. Some countries (e.g., China and Russia) will find economic and social advantage in balancing apparently competing interests—like the need to protect civil liberties while simultaneously exercising quarantines, strict protocols, and activity surveillance—because expectations of privacy will be limited given the state already controls and actively monitors network activity. These and other relatively authoritarian regimes may find "The New Normal" easier to deal with, as it facilitates state focus on a few big targets that really matter while leaving low-level financial crimes behind. Such governments nevertheless will be increasingly challenged by citizen cyber vigilantes, though they may be able to make deals with the largest firms about when and where a private actor can legitimately retaliate.

In contrast, the starker the choice between civil liberties and freedom of expression on the internet, the greater the cost for many Western countries. European countries will find they have the furthest to pivot, given the entrenched privacy protections and mindsets that will be shaken by widespread transparency. Some may respond by restricting internet access at the point of the consumer/citizen, rather than risking a wholesale loss of privacy. New cleavages may also arise, for example between the Cold War generation insistent on strong privacy and younger generations that have never experienced such privacy and see less value in it.

International dynamics will be further complicated by the growth of "hacker haven" countries that seek to legitimize their own position in the world order. Hackers will provide these havens with a new income stream that will invigorate local economies. Yet that income may fluctuate wildly or dry up as more data is made public; those havens that track high-end resources and provide a home for the most sophisticated criminals will have a greater likelihood of achieving economic stability. Over time, the trend toward making nearly all data public may become a rallying cry for haven legitimation in some places. Hacking revenues are licit, havens will argue, given the realities of the internet. After all, you can't steal something that is already free, and the essence of entrepreneurialism is creating value from cheap (or free) assets—legitimately or otherwise.

It seems likely that terrorist organizations (groups like ISIS or its successors) will at first become more prominent in this new world. To the extent that their strategy involves creating a gradual corrosive drag on Western economic power, they will invest a fair amount in cybercrime. But over time, their profits will probably shrink as they are out-competed by the more sophisticated and technologically adept criminals motivated by money more than ideology.

Meanwhile, foreign relations and diplomacy will become a different kind of game, one that has long been talked about in the post-WikiLeaks era but never before realized. Because international actors will no longer be able to prevent foreign companies, intelligence officers, and governments from taking information that has been made public, informal security networks will be constantly at risk of breaking down, and states will no longer have leverage to trade. One end result will be greater overall transparency, for better or worse, on controversial decisions. Foreign partners with lesser ability to protect highly secretive calls and memos will be weak links in the secrecy chain and may get shut out of diplomacy as a result. There will surely be more attempts at international cooperation on cybersecurity issues, but those countries that benefit from the emerging regime will have an interest in slowing down the process, making efforts to cooperate less effective. In this scenario, the hesitaters and blocking coalitions will almost always have the wind at their backs.

THE WAY FORWARD

In this scenario, the internet of 2020 will have evolved along lines that already exist today—but it will feel like a very different place. Commerce, politics, social relations, and the meaning of privacy will have been transformed by digital technologies that make insecurity, not security, the internet's foundation. The last vestiges of techno-utopianism will vanish. Crime (and the ever-present possibility of crime) will color everything that people build, do, share, and learn. Priorities will be set about what absolutely must be kept secure, but only a small number of those priorities will have a chance of holding up. In some cases, data and interactions will be taken increasingly offline. In other cases, users will abandon technology altogether. More than anything, individuals and organizations will try to leapfrog ahead of criminals by letting data become public.

In this scenario, cybersecurity researchers in the year 2020 will wish that researchers in 2016 had been looking more deeply at how different institutions (e.g., government agencies, corporations, and nation states) could adapt to an environment of such vast data insecurity. They—and the public at large—will wish for further clarity about:

TIPPING POINTS

How to identify the tipping points that will lead to a wholesale change in attitudes and behaviors about cybersecurity

HACKER HAVENS

The terms and conditions under which nation states that support international criminal hacker enterprises gain or lose legitimacy

PRIVACY

The shift from privacy as protecting data from being released to the public to privacy as preventing the abuse of data that has already been released

BOUNDARIES

The ways in which boundaries for exclusive, secure online communities can develop, and the mechanisms by which those boundaries, once violated, can be restored

INFRASTRUCTURE

The changes in infrastructure—both the legal regimes required to regulate transactions and the training, staffing, and funding of law enforcement—needed to adapt to a world where the internet is both ubiquitous and insecure

Cybersecurity researchers will also need to produce new insight into possible warning signs that this new world of baseline insecurity is indeed approaching, and possibly faster than people think. These warning signs might include increasing weakness in the market for encryption solutions and the growing popularity of new and ever-more complex password protection techniques (or replacements for passwords altogether). Identifying these signs early could help individuals and institutions better prepare for the surprising behaviors and interactions that will emerge in "The New Normal."

SCENARIO 1 FOOTNOTES

1. "The United States' top intelligence official said in September [2015] the greatest online threat isn't a crippling digital strike against American infrastructure—but the near-constant, lower-grade attacks that are carried out routinely." See Elias Groll, "U.S. Spy Chief: Get Ready for Everything to Be Hacked All the Time," ***Foreign Policy***, September 10, 2015, accessed March 21, 2016, http://foreignpolicy.com/2015/09/10/u-s-spy-chief-get-ready-for-everything-to-be-hacked-all-the-time.

2. See Katie Benner, "Apple Confirms Discovery of Malicious Code in Some App Store Products," *The New York Times*, September 20, 2015, accessed March 21, 2016, http://www.nytimes.com/2015/09/21/business/apple-confirms-discovery-of-malicious-code-in-some-app-store-products.html?_r=1.

3. See Marc Andreessen, "Why Software Is Eating the World," *The Wall Street Journal*, August 20, 2011, accessed March 21, 2016, http://www.wsj.com/articles/SB10001424053111903480904576512250915629460.

4. This is a term typically used to describe legal businesses.

5. 18 U.S.C. § 1030.

6. See Kevin Poulsen, "Valve Tried to Trick Half Life 2 Hacker Into Fake Job Interview," *Wired.com*, November 12, 2008, accessed March 21, 2016, http://www.wired.com/2008/11/valve-tricked-h/.

7. Information and communications technology for development. See Nils Gilman, Jesse Goldhammer, and Steve Weber, eds., *Deviant Globalization: Black Market Economy in the 21st Century* (United Kingdom: Bloomsbury Academic, 2011).

8. See Michael Kassner, "Why Government-Mandated Encryption Backdoors Are Bad for US Businesses," *TechRepublic*, July 14, 2015, accessed March 21, 2016, http://www.techrepublic.com/article/why-government-mandated-encryption-backdoors-are-bad-for-us-businesses.

9. See Robert Jervis, "Cooperation Under the Security Dilemma," *World Politics* 30 (1978): 167–214, http://www.jstor.org/stable/2009958.

10. See James Ball, "Cameron Wants to Ban Encryption—He Can Say Goodbye to Digital Britain," *The Guardian*, January 13, 2015, accessed March 21, 2016, http://www.theguardian.com/commentisfree/2015/jan/13/cameron-ban-encryption-digital-britain-online-shopping-banking-messaging-terror.

11. See Lamont Wood, "The Clock Is Ticking for Encryption," *Computerworld*, March 21, 2011, accessed March 21, 2016, http://www.computerworld.com/article/2550008/security0/the-clock-is-ticking-for-encryption.html.

12. In response to government "no fly" list surveillance, one professor made his life a public art installation. Hasan M. Elahi, "You Want to Track Me? Here You Go, F.B.I.," *The New York Times*, October 29, 2011, accessed March 21, 2016, http://www.nytimes.com/2011/10/30/opinion/sunday/giving-the-fbi-what-it-wants.html?_r=2.

13. Jack E. Greene, ed., *Encyclopedia of Police Science* (New York: Routledge, 2007), 112.

14. Robert Putnam, *Bowling Alone: The Collapse and Revival of American Community* (New York: Simon and Schuster, 2000).

15. NPR, "The Thomas Eagleton Affair Haunts Candidates Today," NPR, last updated August 6, 2012, accessed March 21, 2016, http://www.npr.org/2012/08/04/157670201/the-thomas-eagleton-affair-haunts-candidates-today.

16. Underwriters Laboratories (UL) is a consulting and certification company that performed independent safety validations for many new technologies in the 20th century. Underwriters Laboratories, "History," accessed March 23, 2016, http://ul.com/aboutul/history/.

For more information on the Center for Long-Term Cybersecurity or these scenarios, please visit **cltc.berkeley.edu.**

SCENARIO 2

OMEGA

This is a scenario in which predictive analytics for individual behavior will exceed expectations, becoming different in kind, not just in degree.

With accelerated developments in machine learning, algorithms, and sensors that track human action and enable datasets to feed off one another, the internet of 2020 will have embedded within it profoundly powerful models capable of predicting—and manipulating—a surprising range of human behavior. Rather than infer individual tendencies from trends and groups with similar characteristics, these new models will make truly individualized predictions that are granular, discriminating, and accurate about complex behaviors. The power of data science to predict individual behavior at this very precise level will become the most polarizing debate of the decade: is it an indicator that humanity has handed over its most important powers, freedoms, and mysteries to digital technologies? Or is it an indicator of stunning progress, enabling societies to more effectively solve some of their most recalcitrant problems? While this debate rages on in the abstract, these powerful predictive analytics will generate new security vulnerabilities that outmatch existing concepts and practices of defense, focus increasingly on people rather than infrastructure, and prove capable of causing extreme damage, financial and otherwise.

THE WORLD

In this scenario, the availability of vastly greater amounts and varieties of high-quality data, coupled with advanced algorithms and analytics capable of interrogating that data, will enable highly precise and individualized predictions of human behavior. While today it is possible to predict the aggregate behaviors of groups and populations, in 2020 such predictions will be orders of magnitude more accurate and—most importantly—far more personalized, to the point of predicting the behavior of a single person. In this new world, high-tech firms and sophisticated criminals alike will be able to identify (and, in some circumstances, control) the future behavior of particular people at a surprisingly granular level. Many will regard this capability as a signal of the last—or "omega"—algorithm.[1] Pessimists will see it as the final step before humanity hands over all power to ubiquitous technologies—or even (according to extremists) as an end to free will. Optimists will believe it possible for dynamic individualized predictions to solve problems that humans had almost given up on.

Far from being an obscure debate among abstract philosophical positions, the battle between these perspectives will likely become the defining political and moral cleavage of the decade. Illicit actors (indifferent on the philosophical point) will simply take advantage of these new technologies and the controversies they create to more precisely target and differentiate their attacks, making security even harder to achieve than it is today.

There will be categorical differences between the predictive algorithms of 2016 and those that arise in this scenario.[2] In 2016, algorithms attempt to predict individual behavior by drawing inferences about the behaviors of populations with similar profiles (e.g., white females over 55 prefer to watch *60 Minutes*; therefore, Sue, a white female over 55, likely prefers to watch *60 Minutes*). These algorithms typically express a view of an individual's preferences that translate into probabilistic predictions (there is an 85 percent chance that Sue will watch *60 Minutes* today).

In 2020, next-generation algorithms will be able to skip the demographic shortcuts and narrow in on the specific preferences of a single individual (Sue herself prefers to watch *60 Minutes*). More importantly, probabilistic predictions will become contingent predictions, with tightly accurate statements about the precise conditions under which person X will take action Y. We will know exactly under what conditions (time, place, cost, etc.) Sue actually will watch *60 Minutes*.

Relevant assumptions from traditional microeconomics—for example, that preferences are both stable and transitive—were always imperfect, but in this scenario they will no longer be needed. Probabilistic predictions were always a pragmatic compromise—in fact, Sue either will or will not watch *60 Minutes*, and the 85 percent prediction just meant we did not have a full understanding of the conditions affecting her choice. In this world, the algorithms do understand.

In 2020, next-generation algorithms will be able to skip the demographic shortcuts and narrow in on the specific preferences of a single individual.

Commercial-driven technological development will be a principal driver of this future landscape—but so will the relentless curiosity of human beings to understand one another and themselves. The

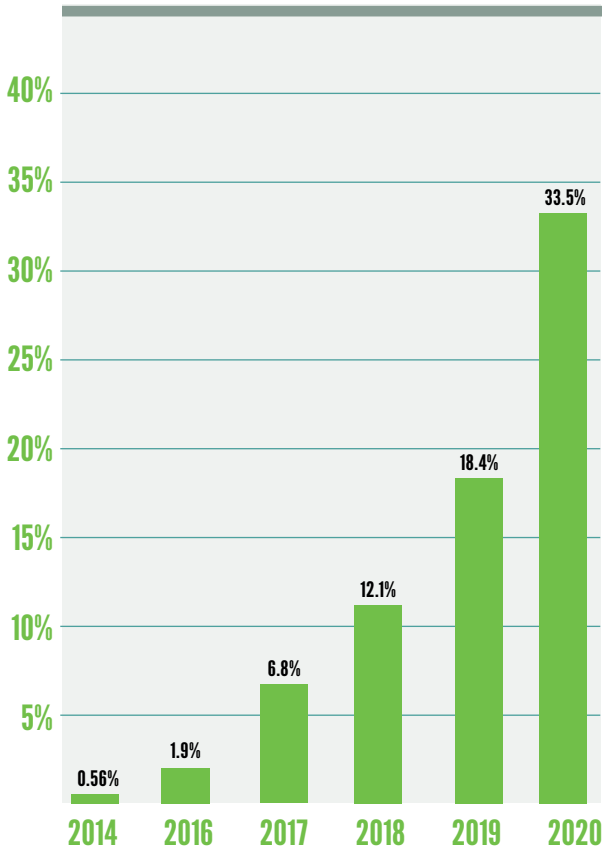
financial returns realized when machine-learning techniques are applied to the prediction of individual behavior will accelerate the technology far beyond what was formerly seen as possible. Cheaper storage, faster hardware, more efficient processing, and advances in simulation and cognitive processing—along with business models and financing—will together accelerate progress. The availability of low-cost baseline predictive analytic infrastructure (the most profitable service from Amazon's cloud in 2018?) will free up researchers to focus their time and effort on developing and testing much more elaborate prediction models. The concept of "big data" will evolve toward rich data, wide data, and then dynamic data. Software will improve to better deal with data types along various spectrums, including modalities, granularities, and temporality. New methods of coding the validity of predictions will become instrumental in improving feedback and learning time. These positive feedback loops will allow models to improve significantly faster than expected. Even some of the more audacious projections for 2020 might be exceeded by 2018.

Businesses, governments, educational institutions, and others will continue to promise extraordinary benefits to those willing to grant greater access to their personal information. Surprisingly, many individuals won't need much convincing. Those not swayed by benefit-cost or benefit-risk calculations about sharing data will be so fascinated by the promise of understanding their own behavioral mysteries that they almost will not be able to resist. No one will have to force the next-generation Fitbits and dry EEG devices and their associated algorithms onto users; users will put them on themselves because they want the results.

By 2020, it will no longer be interesting to categorize an individual as a member of a population class or offer probabilistic assessments of what he

FROM THE FUTURE

TARGETED ADVERTISING EFFICACY INCREASES



A graph showing the click-through rates of ads delivered in mobile apps, for Americans aged 18-34. Note the spike in 2017, which stemmed from the increased sophistication of predictive models and the adoption of shared personal behavior files (PBFs).

or she will do. Instead, the new class of predictive analytics will look at the deep foundation of an individual's decision-making and behavior. As long as data collection is essentially unrestricted and demand for predictability continues to skyrocket, the energy behind this trend will remain extremely strong. Competitive pressure to identify new streams of data will keep building to the point where the marginal returns might start to decline, but who knows where that line is?

In this world, predictive models will play an increasingly significant role in day-to-day life, whether they are used to route global air traffic, choose products for display, or calculate when and where to deploy troops. Weight-loss companies will be able to make precision diet and behavior recommendations based on predictions about when clients will have cravings. Companies will be able to correctly forecast the total sales that would be generated from the European rollout of a new product. In 2020, will CVS Health begin prefilling people's shopping carts, provoking complaints from competitors as it prefills the carts with store-brand products?

How can companies achieve such gains so quickly? For individuals, the core of this predictive model will involve the development of "personal behavior files" (what will become the successor to the "customer information file," or corporate file containing demographic and use data about each individual customer). Personal behavior files will contain detailed information about an individual's past behaviors, including situational information that will help companies understand when and under what circumstances they have acted in the past. The development of such a file may start quite early in life. For instance, parents concerned with tracking the progress of their young children's development might actively support the use of devices that record play behavior and derive patterns related to stress, competition, and the like.

There is an irony in all this. As the ability to predict individual choices and behaviors improves, the ability to predict group behavior will become both less useful and less accurate. Many existing group modeling efforts will feel clunky and become obsolete. Moreover, aggregating individual predictions into group predictions may prove even harder and less accurate than the old approach of disaggregating downward from groups to individuals. Small mistakes (whether in algorithms or in data) spread across many individuals would scale up into potentially big misses at the group level. Whereas today we are generally better at predicting group versus individual behavior, in this scenario the opposite will be true.

For individuals, the core of this predictive model will involve the development of "personal behavior files."

On their own, constrained and contingent individual prediction models will not necessarily revolutionize our way of life. The real discontinuity will be in the meta-models: identifying what aspects of an individual's behavior are predictable and knowing how to use those anchors to contextualize and bound predictions about the rest of an individual's behavior. If these models are not operating effectively in 2020, the possibility will be visible not far over the horizon. With viable models of this kind, individuals could instigate radical adjustments to their behavior through micro-informational interventions and nudges. Put simply, it could become possible to influence a wide variety of individual behaviors by working through a manageable number of key motivational levers. For

FROM THE FUTURE

BILLY
THE BEAR

Looking for the ultimate holiday gift? Billy the Bear is the first toy proven to boost your child's psychological and emotional health!

How? Billy is equipped with sophisticated sensors that can monitor your child's behavior and moods. Parents receive daily updates on their children's well being, along with suggestions for techniques and strategies for improving their emotional state of mind. Best of all, your child's data will be added to his/her personal behavior file, helping create a pathway to long-term health and happiness.

BILLY

some people, the key motivation might be status, power, or money; for others, it might be a spiritual goal or generosity.

Once a person's principal lever is known, the threshold for influencing what he or she does next could be surprisingly low—and this would be just as applicable to illicit and illegal activities as to legal ones. For both attackers and defenders in the cybersecurity world, attention would shift decisively from infrastructure to people. It is common to hear in 2016 that "people are the weakest link in security." In this scenario, that statement becomes a fundamental truth in new and profound ways.

OUTCOMES

The revolutionary idea that defines the boundary between modern times and the past is the mastery of risk: the notion that the future is more than a whim of the gods and that men and women are not passive before nature. Until human beings discovered a way across that boundary, the future was the mirror of the past or the murky domain of oracles and soothsayers who held a monopoly over knowledge of anticipated events.

- Peter L. Bernstein,
"Against the Gods: The Remarkable Story of Risk"

Throughout history, the ability to model, quantify, and subsequently put a price on new categories of risk has transformed uncertainty into an actionable equation and repeatedly catalyzed the remaking of economics, politics, and technology. As we approach 2020, the ability to model, quantify, and price the risk attached to granular actions of individuals—to shine light onto what used to be unknowable at useful scale—will become an essential part of the way the world works, and significantly change the cybersecurity landscape as a result.

The shift from statistical representations of group behavior to individualized predictions will become a major driver of change. The privacy calculations that people make in 2016 when it comes to their Fitbits, smartphones, and connected cars will seem anachronistic, because what you get in return for your data in 2020 will be a new set of insights about yourself that are—as Arthur C. Clarke once said of sufficiently advanced technologies—barely distinguishable from magic.[3] A subset of the population will continue to use Tor and other dark web tools to preserve their anonymity[4] or seek to obfuscate data from search engine queries.[5] But this subset will operate on the margins.

. . . what you get in return for your data in 2020 will be a new set of insights about yourself that are . . . barely distinguishable from magic.

Much like credit scores today,[6] the "answers" that prediction systems provide will appear to emerge from a black box. Only a select number of technical experts will have the sophistication to dissect the new algorithms, the vast majority of which will be neither public nor well understood. Few people outside of specialist firms will comprehend how these algorithms target individual, not group, behavior, or grasp the full significance of that change. For most people, what will be salient are the tangible benefits these algorithms bring.

Consider the example of predictive policing: if predicting individual criminals significantly reduces crime in dangerous cities, the average member of the public will be unlikely to object, even if there is limited transparency about how this new data

shapes policing practices. Would theoretical and philosophical objections to predictive policing put forward by academics and other critics gain any traction with the public? Perhaps in a few European countries with powerful resistance to police intervention, like Germany. Much less so in places like France and Spain that are historically more comfortable with policy autonomy. Almost certainly not in the small, rich autocracies of the Gulf and semi-democratic states like Singapore.

In the United States, the baseline response will be ambivalence. US firms will lead many of the technological and commercial developments that enable predictive policing, but occasional media exposés will constrain just how far local governments go. At the same time, surprising success stories will emerge from "broken" cities that seemed resistant to other means of stopping devastating cycles of crime. The NYPD may be an early leader due to its distinctive license to operate given the perceived risk of terrorism. Overall, the trajectory would point toward greater acceptance of such practices. Algorithm-driven policing would also likely be perceived as more fair than traditional practices, which are visibly subject to racial and other biases. A small number of type 1 errors (false positives) will get outsized attention, but that attention will not be enough to change overall sentiment.

In the commercial sector, many companies will find great utility in this new reality, which will lead to a virtuous cycle as they invest in building software and acquiring data to further improve individualized predictions. The temptation and competitive pressure to participate in this new frontier would be almost irresistible. Data science teams might eventually split into data and prediction teams, with the latter adding neuroscientists, cognitive scientists, simulation specialists, game theorists, and even symbolic logisticians and philosophers of

FROM THE FUTURE

Use of Prediction Models for Law Enforcement on the Rise in Asia

Police forces in Beijing, Shanghai, New Delhi, and Bangkok use predictive tools to deploy forces where crime is "almost guaranteed to happen."

May 5, 2018

Last week, China announced it will commit more than $500 million in training and technology to equip local police to use predictive analysis to guide the strategic and tactical operations of their forces. Yesterday, law enforcement officials in New Delhi revealed that they, too, have started using predictive policing tools. "This software is the future of policing in India," says Aditya Gupta, spokesperson for the Indian Police Services. "It can tell us when and where crimes are almost guaranteed to happen."

Such software, now available from diverse suppliers such as Palantir and Google, matches the individual behavior patterns of citizens (as tracked through license-plate scanners, closed-circuit networks, and other devices) with environmental data (such as broken windows and shifting air temperature) to zero in on city blocks where crimes are most likely to occur next. These cities are following a global trend. Roughly 60 percent of police departments in the United States, the United Kingdom, and Australia already use prediction-based analysis.

Meanwhile, the Chinese government is also using predictive models to guide the operation of its large-scale infrastructure systems, such as water treatment and emergency response. In January 2018, China invested $900 million in a new system that will combine data from more than 500 sources—including smart meters and digital water-usage monitors—to create detailed profiles of households, with a goal to "better deliver services and anticipate usage patterns and possible shortages," according to Zhang Wei, a spokesperson for China's National Energy Commission.

Not surprisingly, human rights and privacy advocates object to the use of so-called personal profiles by police forces, and many have called for stricter limits on how such data can be used. "With these algorithms, we're seeing clear examples of bias in law enforcement," says Li Gao, a human rights activist based in Taiwan.

Others point out that the use of predictive tools by police forces makes the police's own actions more predictable. In December 2017, a team of drug traffickers in Indonesia was caught using a stolen model originally developed by INTERPOL to determine when and where drug-enforcement officials would be based, maximizing their ability to smuggle goods across borders.

science to their rosters. Companies that have long been repositories for thus-far unused datasets would see untapped potential in developing analytic capabilities—and the hiring of in-house analysts would explode.

The temptation and competitive pressure to participate in this new frontier would be almost irresistible.

At the same time, this transition will be tumultuous and difficult. Like the development of web technologies in the 1990s, this new shift will involve not just incremental improvement to existing processes but also the institutionalization of new technologies that reshape terms of competition in many markets. Incumbent-firm advantage will be upended as new firms gain a significant competitive lead in developing and applying predictions to individual customers, clients, and citizens.

These developments likely would coincide with a continued slowing in economic growth rates, not only because of ongoing secular economic stagnation and financial crisis recovery, but also because of the new challenges of operating in this highly granular customer- and employee-segmented world. Consider how firms focused on optimizing business models and applications for large populations will have to transition. In some sectors—public transport, for example—insight into the granularity of individual behaviors will yield significant benefits over population-based predictions. Large firms that were focused on group prediction may have a difficult time switching tactics, such that smaller, local providers are able to assert market power. Would most automobile companies be able to navigate this transition quickly enough, or would they become commodity providers in a transportation market now dominated by upstart prediction firms (perhaps next-generation Ubers and Lyfts) that know, with a high degree of certainty, precisely where and when a person wants to travel from point A to point B? In a sector like education, the ability to create truly customized and individualized curricula and learning systems would run up against longstanding business models, industry structures, and huge incumbent institutions. The market will favor the upstarts because they perform so much better, but the friction will be tremendous.

The geopolitics of this scenario will also present challenges, as next-generation predictive analytics will plausibly be seen as the next major source of power in global political economy and security systems. If prediction technologies evolve quickly along positive feedback loops, then this scenario would most likely reinforce the power of those who start in the lead, implying a new phase of American hegemony. This in turn would engender resistance, such as internet "balkanization" and data nationalism, not so much as an ideological trend or as resistance to surveillance but as a core part of national power strategies aimed at countering US dominance.

Organizations public and private will vary in their ability to keep up in the fierce race for predictive scope and accuracy, spawning a new competitive dynamic between "super-smart" predictive processing and "brute-force" data collection. Put differently, organizations that are particularly strong on the algorithmic side will have somewhat less need for data, while organizations that are relatively weak on the algorithmic side will try to compensate by collecting more data in potentially more sensitive ways. If privacy intrusions or failures of data security occur, it would then be the algorithmically weak that

are more likely to be the transgressors and victims of attack. Traditional goods-producing companies—such as oil companies and TV manufacturers—will likely be in the latter category.

Segmented Cybersecurity: Markets for Predictive Activity

In a world in which algorithms capably predict individual behavior and organizations race to harness that power, cybersecurity will become a segmented enterprise—largely because different realms of human action will not be equally susceptible to predictive algorithms. By 2020, the landscape will divide into three broad sectors, or areas of activity and decision-making, distinguished by the efficacy of predictive models: the strong prediction sector, the throttled (or regulated) prediction sector, and the predictionless sector. The different vulnerabilities that arise within each sector and at the boundaries between them will give rise to an important new cybersecurity agenda for 2020.

Strong Prediction Sector

In this sector, predictions will be highly accurate (well calibrated and discriminating) and reliably available (covering a broad swath of behaviors). This sector will likely include a range of human activity where data is accessible, accurate predictions are monetizable and/or have high significance for governments, and environmental and in-subject randomness is limited. The most powerful and reliable predictive models will develop in areas where all three variables are present, but strong predictions will also occur when any such variables are combined. The private sector will drive developments in this sector most boldly, using "personal behavior files" to help track individual experiences and make predictions based on those experiences.

Healthcare likely falls in the strong prediction sector, as data will be accessible, monetizable, and non-random. Both demanders (patients) and suppliers will see vast promise in what used to be called personalized or targeted medicine—what will now be called (more accurately) predictive medicine. The financial incentives to do more with what today's healthcare companies call "real world data"[7] will continue to mount as insurers and regulators push providers to practice metrics-driven medicine and improve performance on discrete measures, such as hospital readmittance rates. The consolidation of health insurers (driven in part by the Affordable Care Act[8]) will help aggregate customer data at an even larger scale and provide significant revenue streams to fund further applications of prediction-based technology. An aging population in developed countries will contribute on the patient side; baby boomers will see a vast gap between how poorly they are served in the healthcare sector and just about every other sector they touch and are touched by. This generation could very well drive this process forward—to the surprise of anyone expecting higher levels of concern about privacy.

When hospitals are able to reliably complete simple tasks like identifying appropriate individualized plans for each patient being discharged—along with administering programs designed to adjust each patient's behavior through predictive algorithms—the concept of predictive medicine will become real to patients. Importantly, these advances will not be reliant on breakthroughs in genetically personalized medicine; it does not have to be quite so high-science to be effective. Rather, it will be easier to modify at-risk behaviors and develop individually appropriate interventions with well-predicted outcomes that touch on health variables like diet, medication compliance, and social support.

Ultimately, healthcare may become a kind of proof point where the movement toward individualized targeting works visibly to the benefit of sick people, who get better more frequently and more quickly than they have come to expect. The proven benefits would then spread quickly to other markets.

. . . cybersecurity will become a segmented enterprise—largely because different realms of human action will not be equally susceptible to predictive algorithms.

The workplace is another area where all three variables will align for strong prediction. Here, employment contracts, rather than personal trust, grant employers access to data. Companies in 2016 already collect significant data on employees in the name of corporate efficiency; a high-tech office building in Amsterdam will find you the "right" desk and set the room "atmosphere" to your liking.[9] In 2020, enterprises will have moved to entirely new realms of data collection and algorithm investment to predict how employees will behave and perform in the workplace. Firms are likely to redesign workflows, both manual and cognitive, to increase the amount of data available to their prediction models, decrease the amount of environmental randomness, and thus build, act on, and benefit from a range of prediction models on employee productivity. The debate in 2020 will be between companies that use these new insights to help employees succeed and those that are seen as using these insights to weed out and punish—proactively in some cases—less productive workers.[10]

Such changes are likely to accelerate and expand what in 2016 is already a historic debate about labor markets, automation, and inequality, paralleled only by the fights over the rise of labor unions at the turn of the 20th century. Predictions about employee behavior could become the nexus for new problems, leading to calls for stronger social safety nets of a different kind. Some locales may adopt nascent models of prediction-supported employment insurance, while workers' labor cooperatives may take as their primary objective the "breaking" of such models. Will European labor unions take up corporate data collection as their next big point of advocacy?

Meanwhile, many governments will struggle with the adoption of strong predictive technologies. Democratic governments in particular will be constrained by the tangle of existing privacy laws and practices and would likely fall behind compared to the private sector. This could become another front in the outsource-privatization debate; with regard to public-private service delivery—for instance, roads, tolls, and other traffic management—private-sector providers would soon have an unbeatable advantage. Governments may opt to outsource their data and algorithms to the private sector as the path of least resistance to better performance.

Structural tensions also would likely begin to emerge between democratic and non-democratic governments in the strong prediction sector. If the latter cast aside reservations about the new prediction models and use them as a tool for governance, these governments' overall performance could improve in surprising ways. Apart from the political-philosophical arguments this would engender ("Is this the coming golden era for algorithmic-authoritative rule?"), it will also present difficulty for trade negotiations, as those countries most willing to use predictive technologies will

FROM THE FUTURE

http://www.siliconvalleynews.com/linkedin.html

The Silicon Valley **Journal**

Search Go

News | Hot Topics | Columnists | Companies | Special Reports | Marketplace | Tools | Contact | Blog

Predictive Models Help LinkedIn Establish Strong Lead

MAY 12, 2019
MOUNTAIN VIEW, CALIFORNIA

LinkedIn is tapping the vast amounts of data at its disposal to gain insights into the relationships among employees and employers—and is using those algorithms to reengineer the modern workforce.

Companies like LinkedIn have reaped immense benefits from developing algorithms for decision-making in the human resources domain. According to a recent survey in Fortune, nearly 65 percent of Fortune 500 companies now use prediction models for recruiting, hiring, training, and onboarding new workers, and 38 percent use them for analyzing and manipulating team dynamics.

In 2018, LinkedIn released a new algorithm-based service that enables companies to hire complete teams of individuals identified as good matches based on their past employer data and personal behavior files. “Even though the individuals on these teams may have never worked together in the past, they can be carefully selected to reinforce one another’s strengths and fill in any skill gaps,” says Reid Hoffman, LinkedIn’s chairman and co-founder.

In exchange for offering its recruiting services at low cost, LinkedIn retains the rights to monitor the work performance of the new hires it helps place, allowing continuous calibration of the company’s hiring models. The temporary staffing industry has seen a 40 percent decline as LinkedIn has leveraged its data, modeling expertise, and agreements with companies to dominate the HR market.

Meanwhile, the company’s ability to protect its data has come under scrutiny. Last month, a whistleblower at a London-based private equity firm revealed that her employer, Bantham Capital,

used hacked LinkedIn data to identify when workers were most vulnerable to being recruited by other firms, and which individuals were most likely to accept a salary freeze without leaving their jobs.

have structural competitive advantages. Would "non-predictive" economies in 2020 need special dispensations and restrictions, the way "non-market" economies did in the early 21st-century days of the World Trade Organization?

The security dynamic in the strong prediction sector will depend in part on how people respond—in emotional and political-economic terms—to the accuracy of the models and what follows from their predictive capacity. Users will likely find significant value in having increased certainty about decision-making regarding complex and frustrating everyday choices—the effectiveness of a new diet, a workout regimen, a course of study, or personal safety precautions. At the same time, if the surplus generated from these developments is seen to benefit mainly capital and big institutions, then the very accuracy and success of the strong prediction sector could easily become its Achilles' heel by making it the preferred target for disruptive attacks.

Democratic governments in particular will be constrained by the tangle of existing privacy laws and practices and would likely fall behind compared to the private sector.

Consider what it would mean to steal someone's "personal behavior file"—a very lucrative proposition, particularly if the criminal can mine from that file predictions that are not already known to the "legal" market players, or even the actual person behind the file. The simplest spear-phishing attacks could become predictably successful if attackers knew what types of emails a victim is most likely to click on, at what time of day, even as the race against defensive counter-predictions ratchets up.

Vast, quick-profit possibilities here would create a very attractive and highly compensated market for data scientists in the illicit world. Consider the elegance of an integrity attack that introduces a minuscule "bad" argument into an algorithm so that the user of the algorithm receives predictions that completely fail in practice. This could have catastrophic results for the targets. But it would be scientifically fascinating for data scientists to test—particularly for "insider" attacks that might blur the boundaries between what is criminal and what is simply pushing the envelope of scientific research.

Throttled Prediction Sector

In contrast to the (largely unregulated) strong prediction sector, this sector will include industries where government regulations impose more limits on the use of data and predictive models, in order to both manage public expectations and protect against security intrusions. This kind of regulation is likely to develop first in areas where the legitimacy of regulatory action is already established. It is also likely to develop in areas seen as essential to national security, such as defense and intelligence.

Regulations will evolve in order to respond to concrete demonstrations of what in 2016 is referred to as "algorithmic bias" across a variety of sectors, from housing to insurance to education. Arguments about whether human decision-making is more (or less) biased than prediction models will continue to no firm conclusion, and these arguments will create space for policy and regulatory arbitrage, where actors take advantage of differences in regulatory regimes between markets. Copying what Uber did so successfully in the first half of the decade, some companies will defy regulations and legal precedent as they make use of data and algorithms in "throttled" domains, relying on the political power of constituents who desperately want the benefits of the products their algorithms make possible to hold back courts and regulatory authorities. Others will

try more subtle approaches, making small changes to processes and defending against possible legal action only as necessary.

A somewhat peculiar trend in the throttled sector is likely to develop in areas where transparency is already quite high: regulations that seek to limit transparency. Consider public equity markets, where regulation historically has sought to force transparency in order to prevent fraud and other forms of market dysfunction. How would regulations in 2020 maintain equilibrium in the face of massive economic incentives pushing global financial institutions to out-predict competitors' investment algorithms? One (ironic) way to do it might be to limit what kinds of information firms reveal about themselves.

Regulations could also aim to influence the strength of algorithms directly. But this approach will likely lead to other types of regulatory arbitrage where firms hedge their bets by operating in multiple markets. For instance, if governments were to restrict banks from considering certain variables when providing home loans, banks might use that restricted information to make decisions about whether to fund business loans. These kinds of moves will add fuel to the debate about the appropriate role of government regulators, and even whether it is possible to sustain a throttled prediction segment at all.[11]

The security dynamic in this sector would revolve around a game of complexity management. The highly variegated regulatory environment

FROM THE FUTURE

London Times

March 23, 2018

Hackers Manipulate Data to Foil Financial Firms' Data Algorithms

LONDON, ENGLAND – The newly established European Public Prosecutor's Office (EPPO) has launched an investigation into a series of trades linked to a data analysis system used by more than 20 major financial services firms, including many in Europe.

Investigators say that a ring of hackers, most likely based in Malaysia, flooded the internet with vast amounts of subtle misinformation in order to confuse an algorithm, called NASTRAQ, that is widely used by Credit Suisse, Deutsche Bank, and other leading firms to track—and predict—the path of the NASDAQ stock index.

While most data-analysis tools are programmed to analyze financial or economic data, NASTRAQ processes information on a vast scale from every conceivable source, ranging from global news and social-media chatter to election polls, weather reports, pollen counts, and traffic patterns.

EPPO prosecutors contend that the hackers manipulated NASTRAQ by flooding the "datasphere" with fabricated quotes and financial numbers, all hinting at signs of a coming oil shortage. This "news" was translated into 120 languages, dispersed through digital channels, and replicated across more than 10,000 news aggregators—all without a human hand. The algorithm also disseminated tweets and Facebook posts suggesting brewing conflict in the Middle East, and created publicly searchable databases of bogus corporate data in a format that NASTRAQ could process.

A human being might have sniffed out what was happening, but to the lines of code that make NASTRAQ tick, all visible signs pointed in one direction: the price of oil was heading up. Within an hour, 15 major financial services firms bought nearly $300 million worth of oil futures, financial regulators observed the sale of $500 million worth of futures by several banks in Southeast Asia, and the hackers had reaped nearly $20 million in profit.

"People used to talk about 'big data,' but five years ago, we didn't know what 'big' really meant," says Glenda Zapata, a computer scientist at Oxford University. "We're at a place now where the ability to leverage predictive analysis and machine learning is taken for granted. Criminals and regulators alike are all playing the same game: whoever has the most sophisticated algorithm wins."

would, in practice, present an attack surface filled with pockets of vulnerability that are fine-grained and specific. Large-scale attacks may be somewhat more difficult in this environment, but smaller-scale attacks could be much more interesting to invent and harder to detect. The larger, better-funded, and more scientifically sophisticated states and criminals will have an outsized advantage in this world: the capacity to identify and understand arbitrage possibilities will be hard to achieve yet extremely lucrative.

In places where parastatal attackers dominate (China, Russia, possibly Iran), it will likely be the case that the best capabilities are found in large, semi–state-owned enterprises that further blur the lines between military and commercial cyberattacks. For Western governments that would prefer to sustain clear lines between commerce and intelligence, between strategic and corporate espionage, and between civilian and military operations, this blending and blurring will not be a good thing—but how can it be stopped?

Predictionless Sector

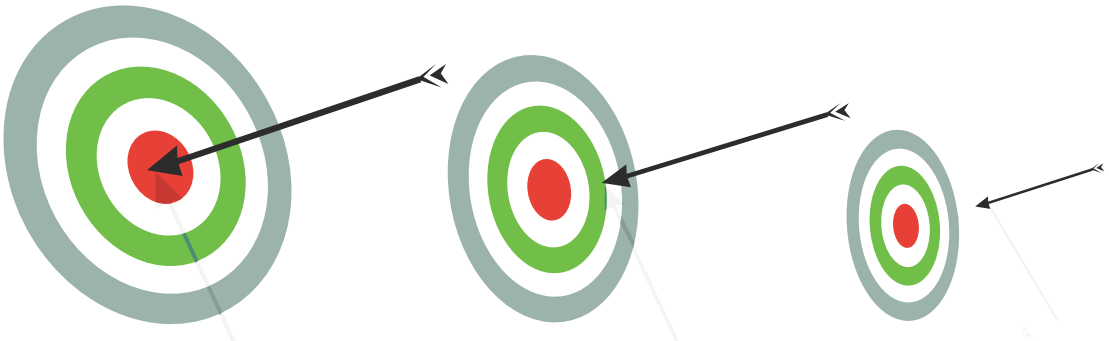
Finally, the predictionless sector will include industries and institutions where data is limited and/or environmental randomness is high, as well as those where the ability to monetize predictive technology is less obvious. It may turn out that human decision-making and behavior in particular realms are predominantly random and simply cannot be predicted. It may just as well turn out that decisions are not yet predictable in 2020 using existing mechanisms, either because the relevant data points have not been identified yet or because they cannot be accurately measured.

Some types of behavior will fall surprisingly fast out of this sector and some realms will be stubbornly resistant to prediction (for example, the results of a competitive team sports event on "any given Sunday"). But whatever does make up this sector at any given moment will have a unique feel to it: when much of human activity can be predicted, the pursuit of what cannot be predicted becomes a sign of privilege, daring, or both. The most ambitious criminal enterprises—not to mention risk-tolerant investment vehicles—will prefer to operate within the predictionless sector. Some may operate in this area because their actions more easily remain hidden; others will do it to capitalize on asymmetric information advantages in this space.

. . . the predictionless sector will include industries and institutions where data is limited and/or environmental randomness is high . . .

The cybersecurity attack dynamics in this sector will be distinctive, because they will focus on a next-generation approach to the strategic manipulation of uncertainty and doubt. Attackers might send deceptive signals about breakthroughs in prediction modeling in order to destabilize others' strategies in (ironically) predictable ways. They might also focus their efforts on small manipulations of data, since the inability to predict makes it unlikely that such small manipulations would be identified. For example, without a reliable model of how people set the temperature in their homes, an attacker could raise the set point on a million connected thermostats by a tenth of a degree without much risk of the data manipulation being caught. Attackers might further aim to introduce noise and randomness in order to foil emerging prediction models that threaten to destabilize their strategies. They might also try to shift the predictive power of targets of interest from the strong prediction sector into the predictionless sector by finding ways to deny access to the data that the models require.

PREDICTIONS: FROM WEAK TO STRONG



STRONG PREDICTION SECTOR

Predictions are highly accurate, reliably available, and discriminating; the potential for environmental and in-subject randomness is limited.

Examples: Healthcare, workforce

THROTTLED PREDICTION SECTOR

Regulations have been imposed to prevent unjust use of predictive models.

Examples: Credit bureaus, housing, employment, law enforcement

PREDICTIONLESS SECTOR

The availability of data is limited, monetization is difficult, and/or environmental randomness is high.

Examples: Risk-tolerant hedge funds, criminal enterprises

Cybersecurity Uncertainties and Challenges

In this world, human behavior will become the key to cybersecurity. While organizations will have much better information about the wants and needs of individual people, the very fine granularity of that knowledge will make it challenging to achieve economies of scale. How, for example, does one build a platform for a political party in mass movement democratic politics when all the micro-differences among people's desired policies are plain to see?

Criminal enterprises will face similar challenges as they too look for new sources of effective scale in their attack strategies. One approach would be to seek to identify and gain access to a small number of very important people in a particular setting—the CEO or the president, the prime minister or the five star general. This (ironically) might mean a decline in very large-scale data theft: why bother with all those "weeds" when you can invest your resources much more efficiently in tending the few "roses" that can get you what you want? It might also lead to a segmentation of cybercriminals, with those who cannot play in the top-notch prediction attack game (in other words, those without the expertise to write or manage complicated algorithms) remaining focused on stealing data. Large, rich, scientifically sophisticated state actors are more likely to land in the former category.

In this world, private corporations will be out ahead of government agencies and regulators (at least in democratic governments) in managing the segmented prediction system. Companies will have stronger incentives and fewer constraints on the use of predictive algorithms, as well as greater freedom to experiment with what can be achieved when the algorithms are throttled or fail. As a result of these incentives—and the value that the illicit economy will place on undermining them—new kinds of security mechanisms will likely be developed that operate across the three sectors. Industry watchdogs—independently funded or in some cases owned and funded by industry consortia—would

be used to validate claims of prediction quality, perhaps through a kind of escrow-based access to the underlying algorithms and datasets. Some governments might also create or "charter" third-party validators or industry self-regulatory bodies in order to gain insight and some oversight at the margins. Either way, firms that underperform and cannot predict to standard will be pushed out of markets rather quickly, which will of course increase the stakes for a successful attack that could quickly bring down a competitor.

It is nearly certain that prediction technologies will quickly find their way into direct military applications as national armies push the boundaries of human performance in conflict. They will also be intensively investigated and in some cases used by intelligence agencies. It has long been the stuff of spy fiction to know enough about particular individuals that recruitment, counter-intelligence, disinformation, and manipulation become extremely precise and targeted science. The most advanced intelligence agencies might not believe it fully possible, but they will boldly experiment nonetheless—if for no other reason than to assess the breakout possibilities open to other, less scrupulous intelligence agencies that might not be willing to play by any set of rules. Might government security agencies even seek to limit the export of algorithms, machines, and people that bolster these capabilities? Surely some governments will try, creating seductive opportunities for "smugglers" and embargo breakers to earn outsized profits in a new kind of cyberpiracy.

The words "surveillance" and "privacy" would come to have quite different operational meanings in this world. When firms and governments can predict what people will do, it will become less necessary to surveil them in a conventional sense. The better the prediction model, the lower the data requirements, and the less the (familiar forms of) intrusion on privacy. Some states—the UAE and Singapore, perhaps—will wholeheartedly invest in what might then be called predictive surveillance, taking advantage of this new equation to reduce visibly intrusive data collection. Might London—probably the world's most surveilled city— follow?

These are some of the questions that will emerge if privacy continues to mean basically what it does in 2016. But what if the "privacy" agenda is forced up a level of abstraction toward profound issues of human autonomy and freedom from coercion, as might occur across much of Europe? At least part of the cybersecurity agenda would then shift toward system-wide government throttling: imposing constraints on what can be done with prediction models as well as deterring illicit actors who, for monetary or ideological reasons, would seek to break those constraints. In some areas of behavior, the confidentiality of predictions per se—even more so than the underlying prediction models—would need to be protected. But the integrity of data-driven models would be complicated to assess and defend. What obfuscations should or would be considered "attacks" on integrity? Would authorities in some jurisdictions call for anti-circumvention laws that mirror what the US's Digital Millennium Copyright Act did for copyright protection?[12]

Ultimately, an operational notion of cybersecurity in this world would need to account for the (possibly monopolistic or at least anti-competitive) power that could be generated by firms with far-reaching prediction models, particularly those subject to positive feedback learning effects. Governments will be less concerned about the dominance of advertising markets than the de facto ownership of markets for aspects of human life. They will need expertise at a very high level to achieve any meaningful visibility into how prediction models are evolving toward these thresholds. Most likely, they will participate actively in the same kinds of modeling in order to understand what the private sector is doing. Who, then, can regulate the regulators in this world?

FROM THE FUTURE

http://www.wikileaks.org

Wikileaks

Search Shop Donate Submit

FOR IMMEDIATE RELEASE
Sept, 22, 2019
Contact: Anne Jones, 202-556-6798

Press Release:
Wikileaks Reveals Use of Predictive Technology by DOD

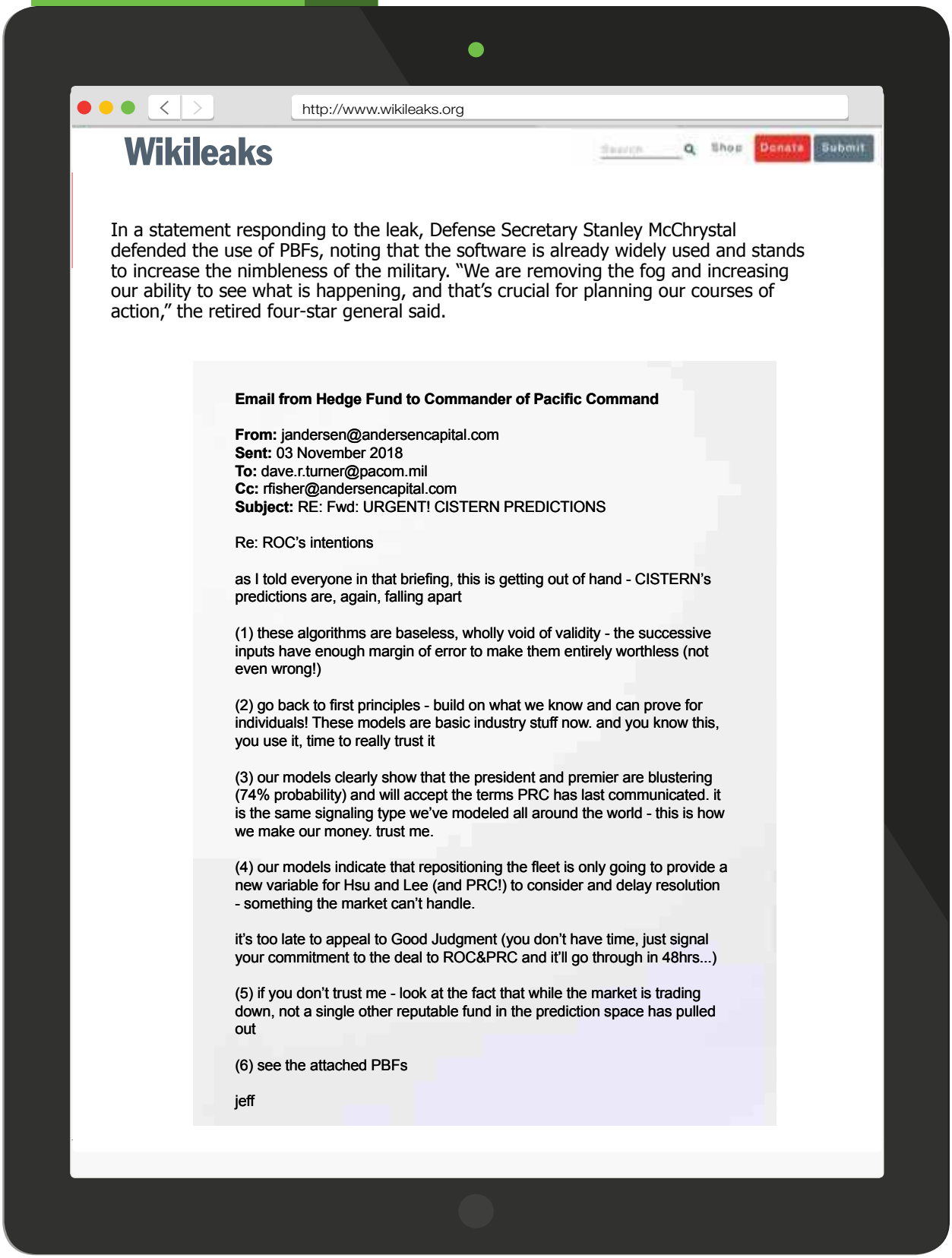
Washington, DC – The US Department of Defense (DOD) and intelligence community have made extensive use of personal behavior files (PBFs) to make predictions about the actions of foreign government and industry leaders, according to documents released by Wikileaks.

The new trove of documents suggest that the US government applied private-sector data analysis tools, most of which rely on real-time analysis of personal behavior files, to generate highly accurate predictions about the behaviors and decisions of leaders from more than 100 governments, corporations, and non-governmental organizations.

The documents indicate that US agencies have also used PBF-based predictive software to influence the recruiting, training, and promoting of leaders in foreign militaries; identify and train foreign agents; organize strategically timed coordinated exercises with foreign armies; and inform key areas of defense strategy. PBFs have even proved useful when dealing with governments such as China that do not permit prediction technology, as the data analysis tools can be adapted and refined to integrate data from a variety of contexts.

Some analysts were surprised by the widespread classified use of PBFs following the embarrassing 2018 failure of the CISTERN program, which "sought to demonstrate the positive impact of ubiquitous data collection," according to the National Security Agency's website. CISTERN had high rates of error, and in some cases led to embarrassingly faulty decision-making, as when the US Army mounted an attack on an empty village in Kazakhstan in December 2017.

Among the documents released by Wikileaks was a scathing email sent by hedge-fund manager Jeff Andersen, who holds stakes in several privately managed prediction firms, to Admiral David Turner, commander of the US Pacific Command, during the November 2018 treaty negotiations between China and Taiwan. Andersen chided Turner for favoring the government's weak algorithms over more effective options available from the private sector (see attachment).



In a statement responding to the leak, Defense Secretary Stanley McChrystal defended the use of PBFs, noting that the software is already widely used and stands to increase the nimbleness of the military. "We are removing the fog and increasing our ability to see what is happening, and that's crucial for planning our courses of action," the retired four-star general said.

Email from Hedge Fund to Commander of Pacific Command

From: jandersen@andersencapital.com
Sent: 03 November 2018
To: dave.r.turner@pacom.mil
Cc: rfisher@andersencapital.com
Subject: RE: Fwd: URGENT! CISTERN PREDICTIONS

Re: ROC's intentions

as I told everyone in that briefing, this is getting out of hand - CISTERN's predictions are, again, falling apart

(1) these algorithms are baseless, wholly void of validity - the successive inputs have enough margin of error to make them entirely worthless (not even wrong!)

(2) go back to first principles - build on what we know and can prove for individuals! These models are basic industry stuff now. and you know this, you use it, time to really trust it

(3) our models clearly show that the president and premier are blustering (74% probability) and will accept the terms PRC has last communicated. it is the same signaling type we've modeled all around the world - this is how we make our money. trust me.

(4) our models indicate that repositioning the fleet is only going to provide a new variable for Hsu and Lee (and PRC!) to consider and delay resolution - something the market can't handle.

it's too late to appeal to Good Judgment (you don't have time, just signal your commitment to the deal to ROC&PRC and it'll go through in 48hrs...)

(5) if you don't trust me - look at the fact that while the market is trading down, not a single other reputable fund in the prediction space has pulled out

(6) see the attached PBFs

jeff

THE WAY FORWARD

In this scenario, the world shifts away from group-based data predictions toward individualized predictive models. Such a shift, which could go largely unnoticed (or be poorly understood) by the public, would occur as a result of improvements in data collection and interpretation. In some areas, predictions will become a significant driver of public life. In others, limitations in data or models—or regulations that inhibit their use—would restrain their impact. But in all cases, new vulnerabilities would arise as a result of the power of predictive modeling, both from malicious actors who socially engineer more targeted attacks and from governments that are ill-equipped to handle them.

In this scenario, members of the cybersecurity research community in 2020 will wish that in 2016 they had been looking at:

PREDICTIVE MODELING

The trajectory of new kinds of security attack vectors resulting from predictive modeling, especially as such vectors displace basic hacking and other security vulnerabilities attracting disproportionate attention today

REGULATION

How predictive modeling can best be regulated, and what schemas of regulation (strict prohibition? licensing?) are likely to be most effective

RISK ASSESSMENT

How human risk assessment operates in this increasingly automated world

OPTIMIZATION

How to determine whether this shift in predictive models might be approaching, and/or identify particular algorithms that use such approaches, in order to rein in dysfunctions that result from such models and/or spread the benefits of such models more broadly

Researchers in 2020—particularly in the social sciences, but really anyone using data science or advanced statistics—might also have hoped to foresee the ripple effects they could face when the modeling of human behavior shifts to focus attention on single individuals and their particular actions, rather than populations or groups that share characteristics.

SCENARIO 2 FOOTNOTES

1. Revelation 22:13 ("I am the Alpha and the Omega, the first and the last, the beginning and the end.").

2. Predictive algorithms (those that attempt to determine an individual's future preferences or behaviors) differ from post hoc algorithms (those that can identify what an individual has already done in the past). We focus here on the former.

3. Arthur C. Clarke, "Hazards of Prophecy: The Failure of Imagination," in *Profiles of the Future,* Arthur C. Clarke, (New York: H.M.H. Publishing Co., 1962).

4. See I2P Anonymous Network, "The Invisible Internet Project," accessed March 22, 2016, https://geti2p.net/en.

5. See Clive Thompson, "How to Baffle Web Trackers by Obfuscating Your Movements Online," *Wired.com*, November 21, 2015, accessed March 22, 2016, http://www.wired.com/2015/11/clive-thompson-10.

6. Companies are increasingly exposed to similar black boxes; banks are now requiring certain companies in China to have a cloud robot inserted into their supply chain management systems in order to determine whether they are creditworthy. See Deng Yaqing, "Credit by Algorithm," *Beijing Review*, October 1, 2015, accessed March 22, 2016, http://www.bjreview.com/Business/201509/t20150925_800039447.html.

7. The contrast is with RCT (randomized clinical trial) data, which in 2016 is still considered the "gold standard" for life-sciences research purposes.

8. See Anna Wilde Mathews, "Health-Care Providers, Insurers Supersize," *The Wall Street Journal*, September 21, 2015, accessed March 22, 2016, http://www.wsj.com/articles/health-care-providers-insurers-supersize-1442850400.

9. See Tom Randall, "The Smartest Building in the World," *Bloomberg Businessweek*, September 23, 2015, accessed March 22, 2016, http://www.bloomberg.com/features/2015-the-edge-the-worlds-greenest-building.

10. For instance, this may lead to consolidation in service industries, as predictions about employee behavior and customer expectations unite and scaling becomes more attractive. (The growth rates of some service sectors—constrained at present by the slow and uncertain processes of recruiting, hiring, training, and other dynamics—will increase as prediction models chip away at these stubborn constraints.) In a decade of secular low-growth macroeconomics, the promise of finding replicable and reliable ways to enhance productivity in services that have been historically resistant—and thus subject to Baumol's cost disease (a phenomenon where salaries increase, despite no increase in labor productivity)—will be too attractive to ignore.

11. As in other arbitrage-friendly situations, some will argue that allowing implicit prediction-driven decision-making is worse than explicitly adopting prediction technology; that is, partial regulation will be worse than none at all. In the transatlantic setting, these kinds of arguments will make the Safe Harbor fights that dominated the agenda in 2015 and 2016 look easy to resolve.

12. The DMCA, Pub. L. No. 105-304 (Oct. 28, 1998), criminalizes measures designed to circumvent copyright protection.

For more information on the Center for Long-Term Cybersecurity or these scenarios, please visit **cltc.berkeley.edu.**

SCENARIO 3

BUBBLE 2.0

This is a world in which many of today's data-intensive internet companies—and the neutral platforms and advertising revenue underpinning them—collapse as a result of perceived overvaluation.

An equity market rout follows, with valuations plummeting along with profits. The data that these firms collected will be among the few recoverable assets. Datasets will be stranded in bankruptcy proceedings, sold off in fire sales, auctioned, bought by governments, or stolen. As a result, an open market for datasets will arise in which both licit and illicit players race to gain ownership of these time-sensitive, underpriced, but (potentially) high-value assets. It is a "war for data" under some of the worst possible circumstances: financial stress and sometimes panic, ambiguous property rights, opaque markets, and data trolls everywhere. As a raucous market for data evolves at the intersection of value and security, an equally interesting market for the (underpriced) human capital to work with that data will develop. In both the licit and illicit worlds, pressure will mount to find ways to generate returns quickly and aggressively while protecting them along the way. Cybersecurity and data security thus become inextricably intertwined.

THE WORLD

This scenario grows out of the next great financial disruption, which this time will be focused on data. The prelude to such a crash has already occurred—at least three times—in the modern internet era. First was the circa-1990 end-of-Cold-War recession that shook up the defense sector and led to the market release of both technology assets and a trove of hungry and opportunistic engineers. During the mid- and late-1990s, the first-generation World Wide Web drew on these underpriced assets to create new firms and business models. These dot-com firms, in turn, underwent their own major financial disruption around 2000. That recession released another tranche of engineers, along with underpriced assets ranging from fiber-optic capacity to intellectual property. These were the foundations of Web 2.0. The 2008 "Great Recession," which had roots in structured financing around the housing market, was not set off directly by internet economics. But the value destruction and market disruptions that followed in the wake of this crash similarly drove many weaker IT companies into bankruptcy, releasing assets for cheap acquisition and contributing to the growth of a new generation of internet companies.

From these disruptions, a pattern emerged. In a cyclical manner that invokes an accelerated version of Carlotta Perez's technology cycle logic,[1] financial disruptions spawned new players that buy or use valuable inputs at fire-sale prices. They then leveraged these inputs to create innovative new business models, particularly when governments (anxious to rekindle growth) subsidized them with money and regulatory relief.

In late 2015, the conventional wisdom was that this cycle had been suspended or perhaps overcome by the "real" business models of data-intensive firms that emerged in the new millennium.[2] In 2016, question marks started to arise over that hopeful view. This scenario makes clear in the not-so-distant future that the conventional wisdom of 2015 was wrong and the question marks of 2016 fully justified.

In a "Bubble 2.0" world, slow-moving trends already underway and visible will set the stage for a third internet business model crash. Engineers will start abandoning the high-priced Silicon Valley world for alternative clusters in Singapore, China (Beijing), South Korea, and elsewhere (or perhaps virtual clusters spanning these and other well-connected cities). This exodus will be in part driven by brewing ideological disillusionment within the tech community and broader society about the Valley's product mix ("When did we stop trying to change the world and instead just make indulgence products for rich 30-year-old singles?").

The value destruction and market disruptions that followed in the wake of [the 2008 Great Recession] similarly drove many weaker IT companies into bankruptcy, releasing assets for cheap acquisition.

In Europe, there will be increasing pushback against digital overreach in the privacy and public services realms. Political coalitions similar to the anti-Uber movement and the antitrust movement against Google might form, giving European resistance to the tech revolution more velocity, scope, and credibility. Even in Washington, DC, skepticism will grow about the regulatory arbitrage game, in which companies take advantage not of price differentials per se,

but of differences across markets and regulatory regimes. (Consider Uber's argument that it is not a taxi service, but a platform for likeminded people to meet and "share" rides.[3]) Regulatory arbitrage is already a key driver of super-charged growth, both in scale and geographic scope, among many platform businesses. However, rising skepticism, regulatory realignment, or simple blockage in some geographies will significantly complicate the growth and profit projections that have pushed these firms toward extraordinary price-earnings ratios on public equity markets. It will become more common to hear arguments that these valuations represent a financial bubble about to burst.

With macroeconomic concerns about stagnation in the broader economy continuing to mount through 2016, the word "innovation," which had carried so much political-economic clout in national capitals and on Wall Street, will begin to feel tarnished, and might even start to take on a negative valence. (Will the phrase "innovation wash" be used in the tech sector the same way people use "green wash" in the environmental sector to describe the triumph of marketing over reality?) A gradual shift in market psychology will brew just under the surface, as valuations of data-intensive companies continue to mount. The feeling will grow that investors had yet again built "castles in the air" on a fragile and corroding foundation.[4]

As often happens in markets, it could be an exogenous shock that turns these rumblings into a crisis. A seemingly unrelated concatenation of events—a contested presidential election in the United States, a ratchet-up of violence in the Middle East, a dramatic rise in oil prices—might lead to a sharp fall in confidence. Or it might be the underperformance or even failure of a single iconic firm. Whatever the shock, a slew of earnings reports showing a decline in mobile and desktop advertising revenue among major firms, including Google and Facebook, might exacerbate the downward trend. Within a short period, the market capitalization of big and small technology companies alike could collapse—declines on the order of 50 or 75 percent would not be out of the question.[5] When "castle in the air" narratives lose their luster, the carnage is frequently swift and ruthless—and this time would be no exception.

With macroeconomic concerns about stagnation in the broader economy continuing to mount through 2016, the word "innovation" . . . will begin to feel tarnished.

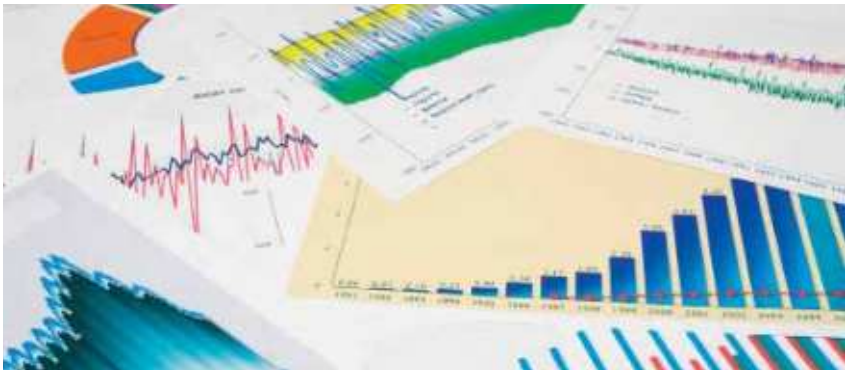
A significant and sustained decline in the valuation of major tech companies would deepen concerns that even the most visible firms have few real and defensible assets above and beyond their datasets. Many believe that the market capitalizations of these firms reflect not so much the services they provide but the expected future value of the data they collect. When "the market" decides, perhaps in late 2017, that these datasets no longer provide sufficient justification for high valuations, many firms that have grown on the basis of that argument will see their market capitalizations blow up with it. From that point onward, 90 percent tumbles in stock price would be entirely plausible. Cash crises and bankruptcies would follow, as banks and venture investors quickly and brutally pull back funding.

FROM THE FUTURE

AdAdvantage

BLOG POST July 9, 2017 9:14 am

Advertisers Shift Their Spending—and Technology Giants Fall



The growth of the commercial internet to date has been built upon advertisers' quest to capture "eyeballs" by presenting promotional messages—such as pop-up ads, banner displays, mobile display ads, videos, or other content—interspersed into shows, games, and other media.

A recent report by the American Advertising Association (AAA), however, has led many of the nation's largest advertisers—including Coca-Cola, McDonald's, GEICO, Toyota, and Ford—to rethink their strategies. The report showed that only about 1 percent of the ads that companies pay for are viewed for more than a second, and the average return on a dollar of online ad spending is just 84 cents.

"Our research found that the return on investment for most online advertising is actually negative," says James Thurman, president of the AAA. "Unlike in the past, we can see today exactly how well ads are performing in all metrics. And it's not good."

The AAA's report may represent the nail in the coffin for dozens of online companies that have struggled to sustain their growth. Similar to the dot-com bubble burst of 2000, most of the latest "pops" are coming from Silicon Valley, where more than 50 tech firms have collapsed in the past 14 months. Housing prices in San Francisco have fallen to 2008 levels, and software engineers are seeking work in Singapore, Beijing, South Korea, and other tech hubs.

This is a well-understood financial panic dynamic—but that may not make much difference in how it plays out. As the crisis enters full force, people like Nouriel Roubini (or his would-be successor) will declare Yahoo to be this decade's equivalent of Bear Sterns, and Facebook the next Lehman Brothers.[6] Sequoia Capital or its equivalent will release a slide deck titled "Good Times RIP 2.0,"[7] reminding industry insiders of the famous 2008 deck that signaled life support at all costs for that generation of companies. Firms will race to hoard (and find new sources of) cash wherever they can. Survival mode will become the dominant strategy.

Many internet business models that were taken for granted in the first half of the 2010s will disappear. If a company as prominent as Twitter were to announce with no warning that its services will be discontinued as of a particular Friday afternoon, it will feel to many like the end of the third era of internet companies has arrived. A few elite media companies will tighten their paywalls; most would have to double down on sponsored content, product placement, and other revenue sources. Some hardware companies will begin to charge full price for their devices (for instance, Amazon might revoke all special-pricing offers on its Kindle). To reduce their reliance on "monetizing data," service companies will charge higher prices. "Freemium" will become a word of the past, and many of the "free" apps that had been iconic symbols of Web 2.0 will no longer be free.

The logic of firms putting their data up for sale in this situation would be straightforward. If data is the one truly monetizable asset a company has, it makes sense to sell it to raise cash (which Good Times RIP 2.0 will say is the only real option) and survive long enough to figure out what to do next. Even a well-organized market can run into trouble when everyone rushes to sell at the same time. But the market for data—to the extent that it exists in 2016—is decidedly not well organized. On the licit side of the fence, there already exists a vibrant and well-functioning market for specific kinds of consumer information, fostered by companies such as Blue Kai and Acxiom that act as clearinghouses for data about individuals.[8] On the illicit side, there is also a robust market for different types of personally identifiable information (PII), including but not limited to financial information about individuals. In both sectors, however, access to data remains limited in 2016, and the quality and price of data being sold is hard to determine.[9] Even so, criminal networks already show strong demand for consumer data, suggesting that there may be equally strong interest for data in other sensitive areas, such as critical infrastructure, transportation, and national security, once the financial crisis allows them to be acquired.

Many internet business models that were taken for granted in the first half of the 2010s will disappear.

Not all data owned by distressed or at-risk firms will suddenly be for sale on the open market. Some contracts will restrict data resale, with courts intervening in high-profile cases. Companies with physical or other assets will be less likely to engage in data sales, given the uncertainty of the new markets. And for some data—that which gets outdated quickly (the equivalent of yesterday's weather) or is already publicly available (such as most people's addresses and phone numbers)—there may be no market at all. Even so, a significant portion of data about people, companies, infrastructure, and many

other (sometimes unexpected) things will be for sale. Once these datasets prove lucrative for a few early movers, other firms will likely follow.

If it is hard to place a dollar value on data before the market gets swamped, it will become still harder as more and more datasets are put up for sale in rapid fashion. How "good" is the dataset? How "clean"? How timely? How accurate? How comprehensive? What could one do by combining this dataset with others? Answering those questions and attaching concrete dollar values to the answers (price discovery, in economic terms) will be almost impossible under panic selling conditions.

Short-term schemes for valuing data would pop up from many places in a competitive manner. Some schemes might differentiate among concrete categories of data assets, such as PII vs. real estate vs. national security vs. financial. Others might try to establish differential value according to human demographics or behaviors. It is unlikely that any of these schemes would stabilize by 2020; instead, data assets would get further jumbled up and confused. The market for data will be tumultuous, volatile, semi-opaque, prone to rumor and cascades—and at the same time, impossible to avoid.

Of course, the great data market explosion of 2017 (or soon after) will not be uniformly bad—not for web users nor for data scientists, and not for the organizations buying and selling data. Optimists will make the argument that data assets were actually more valuable than Web 2.0 firms had understood, and that, by releasing them from their lock-up in retrograde advertising-based business models, a whole new generation of productivity and value—and a Web 3.0 that takes advantage of these new assets—could be created. Whether that kind of

FROM THE FUTURE

NEW YORK TRIBUNE
EDITORIAL

Make Data Research Fair

The recent uproar over "invasive" consumer studies conducted by Uber and Amazon highlights a broader problem with big-data research.

Uber's study used passenger travel data to draw inferences about users' sexual partners, then combined that with purchased health history data and medical purchase data to infer which users were STD-positive. Amazon altered the interactions users had with its Echo device in order to track and study changes in their moods and purchasing behaviors.

These two studies, which various critics have called "creepy," "a fiasco," and "invasive," clearly signal that private-industry controls on ethical research practices are not working. While many academic institutions have internal institutional review boards (IRBs) to review research proposals before they are carried out, most major companies do not. A handful of private for-profit IRBs exist, but their track record is mixed at best.

Moreover, major companies are becoming more protective of their data, often demanding that outside researchers sign nondisclosure agreements before publishing their results. Many datasets—particularly those with personally identifiable data, children's data, and health-related data—are priced so high that only the most well-funded universities can afford them. Less expensive datasets are often too outdated to be useful.

So how can data research be more ethical and less creepy? One solution is to create a system of industry-standard IRBs that are as rigorous as those in academia. While this may require significant financial investment, coordination, and education on the part of companies, it would keep the control of data firmly in their hands.

A second—and preferable—solution is to implement a system of "data fair use." The cities of Oakland and Chicago have led the way on this, requiring a data fair-use clause in contracts with private companies that provide city services and collect citizens' data. Under those agreements, companies are allowed a brief period of exclusive access to data before it enters the public domain. During that exclusivity period, members of the public may still be allowed to run operations on that data, even though they cannot see the content of the dataset.

An industry-wide fair-use system would allow university researchers, working under their institution's IRB, to conduct data research. This increased access to data might unleash the power of nonprofit organizations and nongovernmental organizations to once again make use of data insights and analytics. Either way, consumers are calling for changes in the way data research is done, and they want those changes to be implemented soon.

optimism proves right or wrong in the long run, the short-run dynamics certainly would not feel positive. There will simply be too many datasets of uncertain quality and unclear source flooding a poorly organized market all at once—almost the definition of a fire sale.

Economists might label this a Coase-theorem moment, when property rights dramatically reset around valuable assets, and those assets then redistribute themselves toward the actor that can create the most value with them. In other words, it could be a moment that encourages economic efficiency.[10] But the Coase theorem works only when property rights are clear and transaction costs are low—and neither of those conditions will fully hold in this world. Grabbing at the assets will be an unconventional mix of actors—not just private firms but governments, criminals, intermediaries, and academic institutions—hoping to maximize their value. When a massive amount of what used to be "captive" data escapes into raucous markets, the only certainty is that it will be put to uses that no one expects.

There will simply be too many datasets of uncertain quality and unclear source flooding a poorly organized market all at once—almost the definition of a fire sale.

OUTCOMES

Because this is a market-driven scenario, its primary effects largely fall into two categories: licit market effects and illicit market effects. The tensions and interactions between these two broadly defined spaces—and in the fuzzy boundaries between them—would cause significant secondary effects detrimental to security.

Licit Market Activities

Two foundational principles will drive licit market outcomes in this scenario. First, high-quality datasets have long been hard to come by because they are difficult to identify, very expensive, or simply unavailable. In this scenario, that reality changes partially. For the "right" price, data of all kinds will be obtainable, but the quality of that data will often not be clear. Second, the need for available and functional algorithms that make it possible to analyze complex datasets will multiply far beyond what it is today. After the crisis, the advantage will go to companies that monopolize the talent of top algorithm development, as well as to data and computer science departments around the world.

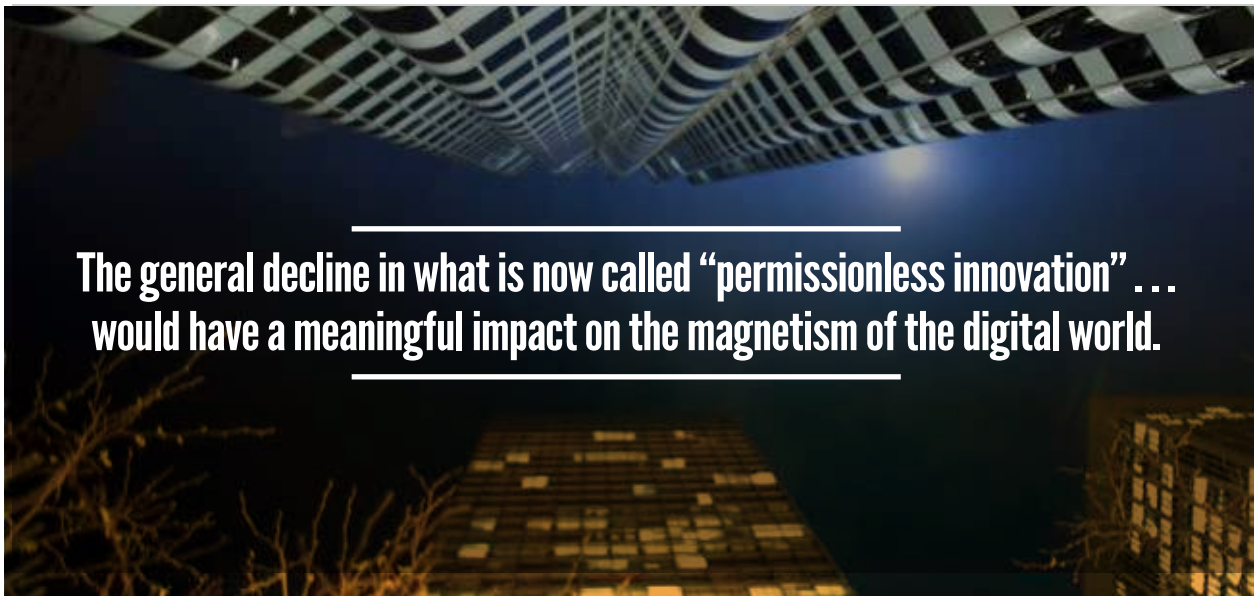
The nontechnical public might find itself with a different mindset after the crash. As investors, they will lose significant money in the stock market crash, as even diversified portfolios will be hit hard by the overvaluation of large technology companies. As consumers, they would find themselves paying more out of pocket for goods and services because the exchange of data no longer subsidizes the costs. Many people will pivot from utter fascination to a sense of disillusionment with Silicon Valley, its innovation culture, and its overall societal impact. Could this extend to a broader skepticism about technology per se and digital technology in particular? While this seems unlikely, the general

decline in what is now called "permissionless innovation" (you get a lot of space, time, and legal license to experiment with new technology applications as long as you can claim "innovation")[11] would have a meaningful impact on the magnetism of the digital world. It might make the average user even more cynical about cybersecurity "fixes" and "investments" as well, precisely at a moment when security will become even more tenuous and important.

What would almost certainly change in this world is the ongoing debate about personal data and privacy. For at least a decade, consumers have engaged in an implied "grand bargain" with the tech industry, giving up their data quite freely on the assumption that their world (and perhaps even the world at large) would change for the better as a result. Privacy activists have tenaciously questioned the value and legitimacy of this bargain, but whether it was a comparatively unregulated deal (in the United States) or a considerably more constrained deal (in many parts of Europe), the privacy agenda never really stuck with the public. That likely will change when core assumptions about what personal data delivers break down.

When the implicit (sometimes explicit) bargain breaks as decisively and broadly as it would in this world, it will feel to many consumers that their data was "stolen" under false pretenses. The legal ramifications that follow could spawn decades of litigation. Perhaps the earliest and most obvious targets would be the click-through contracts and terms of service agreements underpinning much of this data release. The risk of datasets being hung up in litigation would be another constraint on price discovery: who will want to pay a high price for a dataset whose use might be frozen by a court? This might create a price advantage for actors in illicit markets, where calculations of a dataset's value would not be as burdened by concerns about legal usage restrictions.

Tech companies in this world will be driven by the need to generate cash and quickly find new ways to show that data is relevant again. A variety of market response strategies will start to take shape. Small and nonprofit organizations that survive the crisis will be able to access underpriced data assets that they could not have afforded in 2016. This might give a major boost to segments of the pharmaceuticals industry, where "real world data"



BOOK REVIEW: DATA, BOLDLY GOING

Data Trek: Where No Data Has Gone Before
by Mark Craft

259 pages, MIT Press, $23.50

Last month marked the one-year anniversary of the opening of the NASDAQ Data Futures Exchange, which makes the publication of Mark Craft's first book all the more timely.

Using the metaphor of the classic sci-fi series *Star Trek*, Craft charts a "five-year journey" that has brought about "a dramatic shift in how our society conceptualizes and relates to data." He centers his analysis around interviews conducted with figures from inside the "data trenches," including venture capitalists, data scientists, software engineers, insiders from Silicon Valley and Silicon Alley, regulators, investment bankers, and chief data officers.

Drawing upon these diverse perspectives, Craft details some of the key events that brought data to prominence, starting with the "Double December" bubble burst, when Greece exited the European Union and the failure of the ad-based revenue model threw the technology sector into chaos. But as app developers and other companies fell to their knees, their consumer data turned out to be one of their most valuable assets.

He tells the story of Jason Ho, a software engineer at Twitter, who was left jobless after his company's stock collapsed. He recounts Ho's work visa challenges in the aftermath and shares details of the lavish lifestyles promised to many of his coworkers by foreign company suitors. Craft also interviews employees at Uber, which had the foresight to accumulate data at bargain prices, and details the period when ambiguous property rights and lack of regulation sparked "data wars" and unchecked sharing among companies and governments.

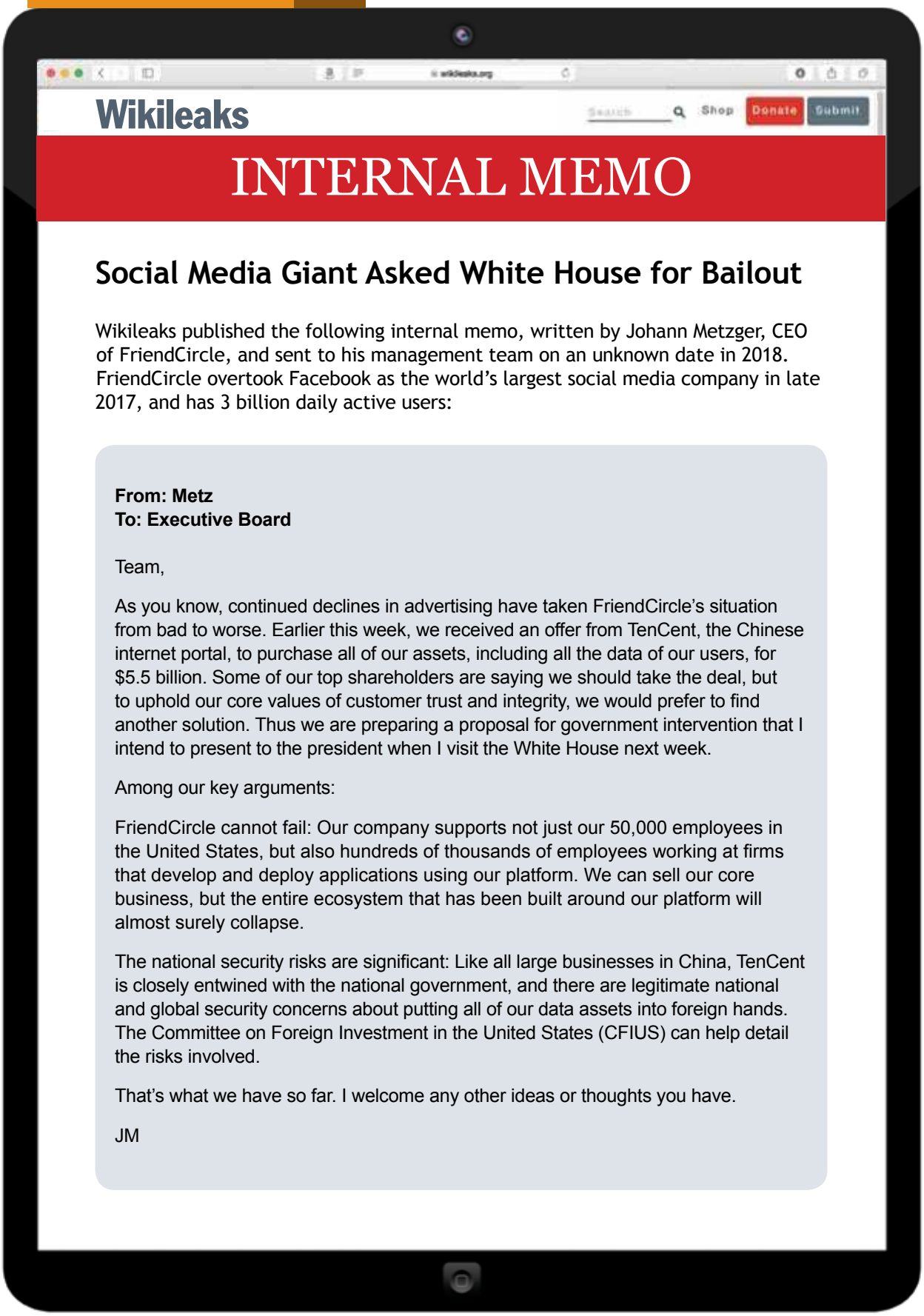
Also included is the enthralling story of Jasper Schultz, the ex-cybercriminal who turned a new leaf once he realized he could make more money with data on the NASDAQ Exchange than selling to private buyers on the black market.

Craft brings the story to a rousing high point when detailing the past two years, when the data trading market became more standardized and regulated, a trend capped off with the opening of the NASDAQ Data Futures Exchange.

Craft's message comes through perhaps most clearly when he discusses the shift toward proprietary datasets and the technical encryption standards that allow the market to know if companies have the data they say they do without ever seeing the data itself. Craft is able to take the mathematics behind what seems like magic and distill it into an understandable metaphor.

The book is a reminder that our current notion of data as an asset is relatively new, and while many of the associated privacy and security concerns have been addressed, we are still standing at the beginning of a much longer journey into wholly unchartered territory.

FROM THE FUTURE



Social Media Giant Asked White House for Bailout

Wikileaks published the following internal memo, written by Johann Metzger, CEO of FriendCircle, and sent to his management team on an unknown date in 2018. FriendCircle overtook Facebook as the world's largest social media company in late 2017, and has 3 billion daily active users:

From: Metz
To: Executive Board

Team,

As you know, continued declines in advertising have taken FriendCircle's situation from bad to worse. Earlier this week, we received an offer from TenCent, the Chinese internet portal, to purchase all of our assets, including all the data of our users, for $5.5 billion. Some of our top shareholders are saying we should take the deal, but to uphold our core values of customer trust and integrity, we would prefer to find another solution. Thus we are preparing a proposal for government intervention that I intend to present to the president when I visit the White House next week.

Among our key arguments:

FriendCircle cannot fail: Our company supports not just our 50,000 employees in the United States, but also hundreds of thousands of employees working at firms that develop and deploy applications using our platform. We can sell our core business, but the entire ecosystem that has been built around our platform will almost surely collapse.

The national security risks are significant: Like all large businesses in China, TenCent is closely entwined with the national government, and there are legitimate national and global security concerns about putting all of our data assets into foreign hands. The Committee on Foreign Investment in the United States (CFIUS) can help detail the risks involved.

That's what we have so far. I welcome any other ideas or thoughts you have.

JM

(RWD) is showing promise for drug development and testing,[12] or to public interest applications like public transport optimization.

Because there will be considerable pressure on new data owners to extract value and demonstrate that value quickly, some sectors (healthcare, for example) would likely see a major boost in competition, subject to first-mover advantage. De-concentration of data from the biggest players could turn out to have a stimulating effect on innovation overall, as newly empowered small firms race to become the next first mover. The biggest challenge for these firms will be to invest adequately to secure their new data assets against criminals, who will be closely monitoring for vulnerabilities wherever interesting datasets land.

Another underpriced asset that would flow into markets—or at least become more "liquid" after the crash—will be human capital: unemployed and underemployed data scientists who, like their defense industry engineer predecessors in the 1990s, will be hungry for opportunities to do great work and make great money. The best of this group will find attractive opportunities designing algorithms to analyze newly available data, but many others will not have the advanced skills needed to engage in algorithmic design. The most pressing question for the remainder, depending on geography and temperament, may be whether the most attractive opportunities lie within licit or illicit/semi-licit enterprises. Some governments will weigh in on that choice with cash and coercion, just as the United States did with regard to decisions made by Soviet nuclear scientists after the end of the Cold War.[13]

As this world moves closer to 2020 and the acute phase of the crisis evolves into its chronic aftermath, new financial instruments will develop to manage the exchange of data assets—for example, data bonds that place claims on the stream of income produced by a dataset over time. As a secondary market in data bonds develops, there will emerge a new and valuable source of information about the perceived value of particular datasets and how that might change (and change hands) over time. Data rating agencies would then emerge to rate both data sets themselves and the repackaged rights to data sitting in bonds or other kinds of derivatives. A futures market on data that is yet to be produced or released to the market—such as data on children that legally must be withheld until age 18—could become a vibrant place to fund new initiatives in data collection. And, of course, there will evolve a vast black market for other types of non-sanctioned data, including all the kinds we know today as well as new combinations of data that offer criminals the opportunity to do damage. For instance, can past shopping preferences help criminals target phishing schemes? Will IP address locations be used to predict when a particular individual will or will not be home?

Governments will have interest in acquiring data not only to save companies . . . but also to ring-fence sensitive datasets that they do not want in the public domain.

Many large firms will have plenty of willing buyers for their data—but the buyers may not always be desirable from a broader political economy and security perspective. One particularly interesting strategic option for large firms might be to seek government rescue, as auto companies and banks did in 2008 and 2009. Could a firm like Google argue that it was "too big to fail"? In an ironic echo of General Motors circa 2009, imagine Eric Schmidt claiming that more than a million US jobs depended on Google directly and indirectly.

The US government will have to listen seriously to these arguments. The economic and national-security policy communities might push for governments to act as "data buyer of last resort." Protecting jobs, maintaining the value of an illiquid "systemic risk entity,"[14] and keeping valuable data assets out of the hands of foreign companies and governments all favor government intervention. The expressed intention, as with GM in 2009, would be for the government to buy up the data assets, hold them through the crisis long enough for markets to stabilize, and then resell them to legitimate private firms on the other side.

In the interim period of ownership, though, the federal government could find itself in a very awkward place regarding privacy and data rights—a much more complicated situation than was the case with GM. Datasets that citizens felt "okay" about Facebook having might suddenly be "not okay" when they are held in escrow by governments, at least in the United States. (In Europe, by contrast, citizens may be more comfortable with governments holding data than with companies doing so.) And what of data about foreign citizens and companies held abroad, particularly those subject to the new transatlantic Safe Harbor 2.0?[15] The US Government would certainly go to great lengths to assure the world that it had only a financial presence in data markets and would not do anything with the data that it now "owned"—but who would really have confidence in that assurance?

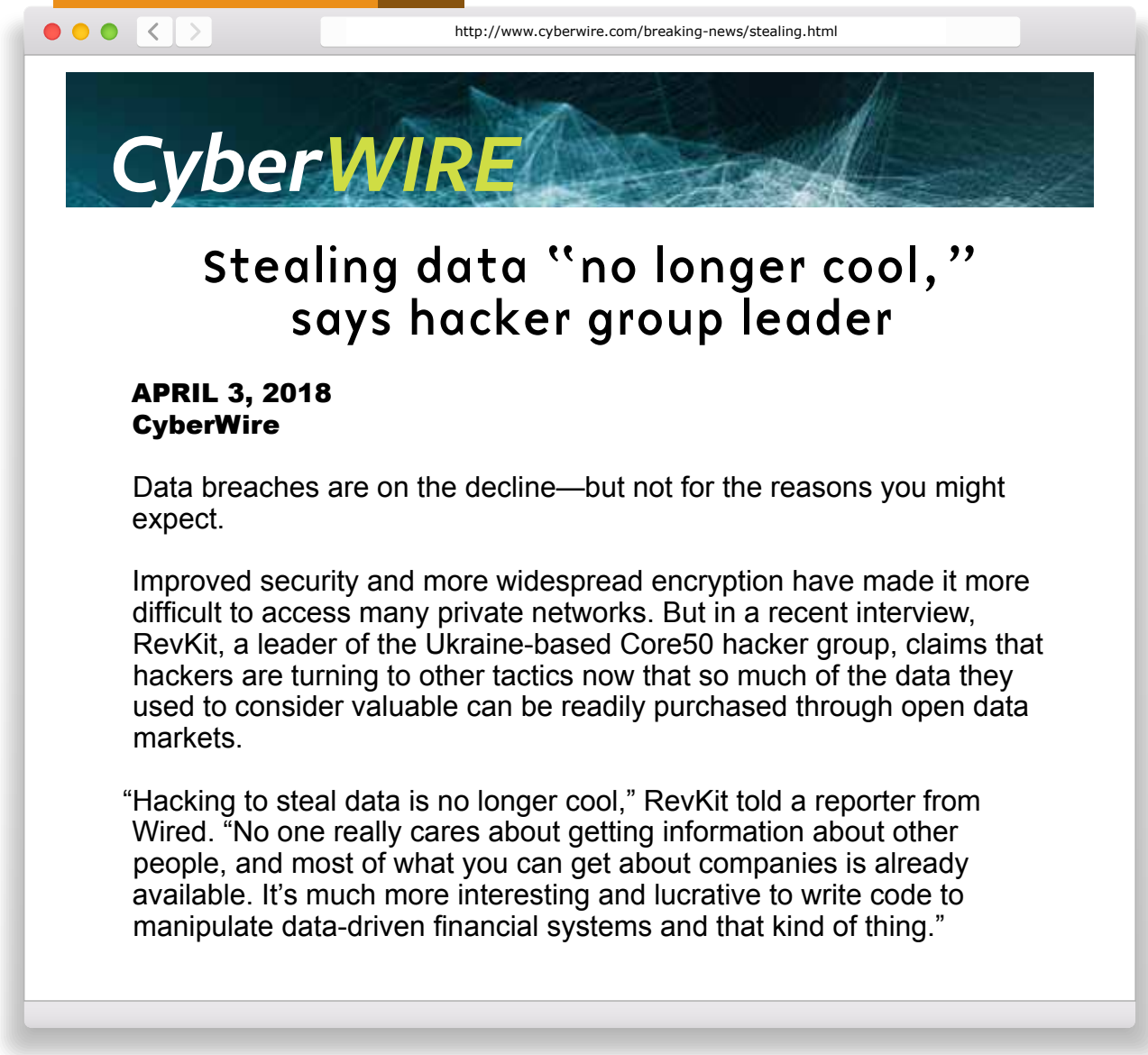
Governments will have interest in acquiring data not only to save companies that might be suffering in the crisis, but also to ring-fence sensitive datasets that they do not want in the public domain. Predictably, governments would be interested in protecting critical infrastructure data and information on government employees. But other categories might be more surprising. Is it possible that data on farm locations and product lines could give rise to a food security question? Could data on top university students be considered a source of leverage in the hands of foreign governments to recruit effective spies? Lobbying in national capitals around these issues would be fast, furious, and intense—as would, potentially, covert counter-lobbying by commercial interests, adversarial states, and possibly criminal networks.

The reset button will also be pushed around beliefs and regulations that pertain to personal data property rights and privacy. As personally identifiable information (PII) is sold to new owners, the people who were the source of that PII will more often than not react with astonishment: "I didn't agree to have my data sold at bankruptcy to a government or firm I've never heard of!"[16] The truth is that in most cases they did agree to it, simply by accepting common terms of service. The fight over such contracts will heat up in new and vehement ways, but it is unlikely to be settled quickly and cleanly. The controversies will be even more difficult to manage when de-anonymization hits combinations of datasets that were thought to have been rendered "safe" through (imperfect) anonymization protocols.

It seems likely that some cybercriminals would switch tactics, finding the licit market more favorable than the illicit.

Governments thus will come under even greater pressure to limit downstream privacy effects. In the United States, the Attorney General's Office and the Federal Trade Commission, among other agencies, will try to keep track of data mobility and restrict the movement of certain types of data. The Committee on Foreign Investment in the United States (CFIUS) will try to prevent foreign acquisitions when national security issues come into play (or when firms are able to make that argument successfully as part of their survival strategy). In Europe, the movement for data privacy will become even more vociferous. But markets will often be moving faster than regulators. Although governments may be able to limit some

FROM THE FUTURE



particularly "dangerous" transactions among large licit entities, regulators will be much less successful in keeping up with small criminal players, who will find themselves with broad freedom of action as they operate under the radar and at smaller scale.

The most important constraints on how licit markets for data would evolve post-crash would be national borders, national regulatory schemes, and national security concerns—a back-to-the-future moment for the "global" internet economy. In 2020, the de facto level of globalization in digital data markets may look surprisingly far below the level of globalization in markets for goods and services.[17]

Illicit Market Activities

Parallel data-market response strategies will take shape in the criminal sector. It seems likely that some cybercriminals would switch tactics, finding the licit market more favorable than the illicit. Imagine the slogan "Who's dumb enough to break into a salvage yard?" floating around hacker websites. Why bother stealing datasets when you can buy them cheaply

FROM THE FUTURE

http://www.cyberwire.com/breaking-news/integrity.html

CyberWIRE

New Data Integrity Certification System Released

NOVEMBER 14, 2018
CyberWire

The Global Federal Data Consortium (GFDC) has released a new certification system to help verify the accuracy and provenance of data, based on its history and record of security protections.

"Data is increasingly seen as a highly valuable commodity, and with more companies selling data to others on the data exchange, there is a need for standards to ensure that any given dataset is unique and authentic," says GFDC director Marc Vermeer.

Leaders from the NASDAQ Data Futures Exchange have signaled support for the new standard, which comes in the wake of last month's disclosure that more than 100 datasets sold on the exchange had been previously hacked and were freely available on the black market.

"The GFDC's certification will make our customers feel secure that the data they purchase is the real deal," says Lindsay McGoohan, the NASDAQ Data Futures Exchange's chief technology officer. "Particularly as we start to sell data bonds, data futures, and other derivatives, it is imperative that we get this right."

on a distressed asset market? Even if criminals sometimes have to set up intermediaries or shell companies to complete transactions legally, the licit market will be seen as a good bargain for many. This would present a major challenge for legal authorities trying to "regulate" as best they could the raucous fire sale. Exactly who is buying the data will be difficult to determine.

In other cases, datasets will become attractive targets for attack and theft. This will be especially true when their new owners fail to take adequate security precautions with their recent acquisitions. How will they make decisions about how much they should invest to protect the data? Criminal groups could grow aggressively by systematically attacking these fresh targets, including both private-sector companies and government agencies that had taken

on data, even if only temporarily as stewards.

Other criminal organizations might offer to act as cut-out intermediaries for governments that seek to buy up certain data assets for national security or competitiveness purposes but prefer not to be identified. Imagine a virtual hacker meeting where participants talk about the possibilities of a "Godfather" strategy: if they could make a deal with a government to look past their previous illegal activities, might they be able to pull off the transformation into legitimate businesses that Michael Corleone couldn't quite finish?[18]

As these data markets become more sophisticated, multilayered, and important, the markets themselves would become an attractive target of attack. Cybercriminals could very well turn their existing tools—physical and network penetration of data centers, denial of service attacks, introducing fraudulent data or noise to manipulate market prices—to these new primary and secondary data markets, as well as the metadata they produce and depend upon. Some criminal activity will also likely become "financialized." Why steal data itself if you can make money more reliably by manipulating the new and untested data-backed financial products and instruments more directly? The geography of attack may very well move toward more traditional financial centers like New York, London, and Tokyo, where data security professionals will also cluster.

Cybersecurity Challenges and Tensions

In this world, cybersecurity and data security will become inextricably intertwined. There will be two key assets that criminals can exploit: the datasets themselves and the humans who work on them. In this environment, the ability to trace the origins of a particular dataset will become critical; proof of "provenance" will become a highly valuable asset. And just as in markets for fine art, falsifying the provenance of data may be a particularly lucrative means of manipulation.[19]

The "price" of a dataset, then, will reflect its value and its overall security characteristics, the same way that in 2016 the price of a house reflects its "inherent" value, its construction and maintenance history, and the crime rate around its physical location. Parallel pricing dynamics will likely emerge in illicit markets as well, with pricing based not only on the inherent value of the data but also on how "insecure" it is—and thus what other illegal manipulation possibilities it presents. In both environments, data with the most security features will become the most valuable. Where and when these markets become relatively efficient (if they do), there would be a de facto regularized price for moving data between the legal and illegal sectors as well.

There will be two key assets that criminals can exploit: the datasets themselves and the humans who work on them.

Sudden job loss for many thousands of tech-industry employees—at least some percentage of whom will be actively recruited by criminal enterprises—will also raise significant security challenges. Governments will be tempted to monitor and try to control the actions of disgruntled or dispossessed data scientists and engineers. They will also seek to preferentially direct these human-capital resources into licit rather than illicit enterprises. This will be an expensive and intrusive proposition with uncertain results.

It may be in the gray areas—the blurry boundaries between legal and illegal, state and private, intelligence and law enforcement, criminal and parastatal, etc.—that the most challenging security predicaments will arise. Consider the likely retrenchment of global communications platforms like Google and Facebook—a tricky situation for

insurgent and terrorist groups (whether ISIS and its successors or extreme-right wing organizations) that use them to communicate and recruit, and equally tricky for the intelligence agencies that track illicit activity. In this scenario, "bad actors" will lose some ability to achieve global scale through a small number of platforms and will have to distribute their efforts across a larger number of smaller platforms. Intelligence agencies will have to track this distributed activity, which means losing economies of scale in surveillance as well. It is unclear who would be advantaged and disadvantaged overall by this dynamic.

The recombination and new sorting of data assets among firms, states, criminals, and others will substantially change the way such actors behave. Many incumbents—who benefit today from their first-mover advantage in the earlier phase— would try to reassert dominance through different means. Others will lose control of their data and possibly their competitive advantage to newcomers. Significant opportunities will emerge for traditional, native, non-data firms (the GMs and Safeways of the world) to transform themselves with a leapfrog move: rather than playing catch-up, they can buy the data assets and expertise they need if they act fast and boldly. Other opportunities will arise for nonprofit organizations and universities, which may want to buy what used to be expensive proprietary data of public or research interest and place it into "open" or "trust" settings. Would organizations like the Marin Agricultural Land Trust set up a sister organization called the Marin Data Trust?

Such a reorganization would create the conditions for an interesting and potentially dangerous multiplayer game between states, criminals, entrepreneurs, and mixtures of each that would be different in important ways from today's dynamics. Criminal networks might be well positioned to make early and ambitious investments in newly available datasets, as their risk-return appetite rises above that of any other actor. Courageous states with lots of capital and economies that would be less, or at least less directly, damaged by the bubble bursting (which might include China, Russia, and Iran) would be presented with attractive opportunities to improve their positions. There would be similar opportunities for capital-rich states that are less active in the cyber and data realms, such as Saudi Arabia, to get into the game. Criminal networks that are not principally digital (like drug cartels) might use this moment to extend their business models aggressively into the data and cyber realms, and those already in the game could go much deeper. Could we see joint ventures between criminal networks and fresh sources of capital—and even the possibility of some such ventures using this moment to "go legitimate" as cyberdefense or digital services businesses?

New attack vectors are also likely to arise as a result of criminals' extensive, in-depth access to data. Blackmail may become the new spear phishing: rather than stealing someone's credential, a perpetrator might force the victim to do the dirty work themselves, on the threat of making their private data public. Of course, such attacks could focus on institutions as well as individuals. Releasing data relevant to ongoing litigation could be as threatening to a company as a web browsing history might be to an individual.

Cybersecurity in "Bubble 2.0" will become a broad landscape in which the political economy of data plays out. Once data is released into highly imperfect markets, its valuation will become the core question that people, organizations, and governments must answer in order to reasonably and rationally set a security agenda. Pressures to act quickly and grab first-mover advantage before data assets become "stale" or are locked up in new ownership configurations will drive the process along much faster than anyone really wants, but it is difficult to see who has the power and influence to slow things down. For consumers, the overall effect may be deep apprehension about financial security, national identity security, and even physical security. (Could, for example, criminals more effectively burgle houses based on geolocation data?) Skepticism would grow that anyone—governments, security firms, or other companies—has the power to alter these volatile, unexpected dynamics.

THE WAY FORWARD

In this scenario, another tech bubble will burst around an overvaluation of data assets. Licit businesses and associated markets will struggle to cope, marking the sunset of previously dominant actors and the entry of smaller players, including from the developing world. Criminal enterprises will grab new opportunities in both the licit and illicit sectors. Governments will become regulators of data sales and purchasers of key competitiveness and national security-relevant data assets, but will fulfill both responsibilities imperfectly.

Cybersecurity in this world will converge even more fully with data security, as datasets, repositories, and data markets become the principal targets of attack. Maintaining security investments during a severe economic downturn (when firms need to hoard cash) creates a challenging dynamic. Investments and capital expenditures will be under pressure, and those that protect against loss, rather than promise gain, will be under the greatest pressure.

In this scenario, cybersecurity researchers will wish that in 2016 they had been looking at:

CRIMINAL CONTROL

How criminal activity would be revalued and refocused in a devalued data market. If criminals can buy a dataset cheaply in a fire sale market and gain legal property rights, would they still bother stealing it

AUTHENTICATION

Techniques for proving the origins of datasets, protecting meta-data against attacks designed to falsify their provenance, and (later) defending against having data collected in the first place (in other words, "privacy-hardened computation").

EFFICIENT MARKETS

What role government might play in creating mechanisms for making markets for data more efficient and secure.20 A murky legal and economic environment in these markets may present as much of a security risk as a direct attack.

HUMAN CAPITAL

Approaches to fostering talent and human capital "security," in order to prevent significant growth and transfer of assets to the illicit sector.

Finally, the US public in particular may wish that researchers had thought more specifically about the second- and third-order consequences of a data-centered financial bubble bursting. Would (mainly) American platform companies flip from being seen as champions of innovation to being the villains of yet another US-induced global recession?

SCENARIO 3 FOOTNOTES

1. Carlotta Perez, *Technological Revolutions and Financial Capital: The Dynamics of Bubbles and Golden Ages* (Cheltenham: Edward Elgar, 2002). Perez argues that there are four stages of technological-economic cycles: (1) irruption (growth of the new paradigm); (2) frenzy (rapid adoption); (3) synergy (renewed economic expansion); and (4) maturity (market saturation).

2. Joint Venture Silicon Valley reported in early 2015 that Silicon Valley economic indicators favored continued growth without "any kind of bubble." See Jeff Elder, "Silicon Valley Is Not a Bubble About to Burst, Report Says," *The Wall Street Journal*, February 3, 2015, accessed March 23, 2016, http://blogs.wsj.com/digits/2015/02/03/silicon-valley-not-a-bubble-not-about-to-burst-report-says.

3. Biz Carson, "Uber: We're Not a Taxi Service, We're a 'Lead Generation' App," *Business Insider*, July 09, 2015, accessed March 23, 2016, http://www.businessinsider.com/uber-fights-california-class-action-lawsuit-2015-7.

4. Burton G. Malkiel, *A Random Walk Down Wall Street: The Time-Tested Strategy for Successful Investing* (W.W. Norton & Co., Ninth Ed. 2007). In May 2015, the *New York Times* reported that "[t]oday, people see shades of 2000 in the enormous valuations assigned to private companies like Uber, the on-demand cab company, which is raising $1.5 billion at terms that deem the company worth $50 billion, and Slack, the corporate messaging service that is about a year old and valued at $2.8 billion in its latest funding round." Conor Dougherty, "Overvalued in Silicon Valley, But Don't Say 'Tech Bubble'," *The New York Times*, May 22, 2015.

5. Volkswagen stock plunged 23 percent after the company revealed it had been cheating on diesel car emissions tests. Naomi Kresge and Richard Weiss, "Volkswagen Drops 23% After Admitting Diesel Emissions Cheat," BloombergBusiness, September 21, 2015, accessed March 23, 2016, http://www.bloomberg.com/news/articles/2015-09-21/volkswagen-drops-15-after-admitting-u-s-diesel-emissions-cheat. LinkedIn stock fell by about 40 percent on one day in early February 2016 following disappointing growth projections. Kathleen Chaykowski, "LinkedIn's CFO: Recent Stock Crash 'Was a Surprise'," Forbes, February 9, 2016, accessed March 23, 2016, http://www.forbes.com/sites/kathleenchaykowski/2016/02/09/linkedins-cfo-stocks-recent-crash-was-a-surprise/ - 62f769724cf8.

6. In 2015, Roubini's chief concern was with "severe market illiquidity" in financial markets. See Fred Imbert, "Investors Beware. A Perfect Storm May Be Coming," *CNBC*, June 01, 2015, accessed March 23, 2016, http://www.cnbc.com/2015/06/01/us-market-timebomb-imminent-heres-why-roubini.html.

7. In 2008, Sequoia released a "Good Times RIP" slide deck for company members of its portfolio, later leaked to the public, urging members to take urgent action to protect themselves from what would be bleak financial times. See Eric Eldon, "The Sequoia 'RIP: Good Times' Presentation: Here It Is," *VentureBeat*, October 10, 2008, accessed March 23, 2016, http://venturebeat.com/2008/10/10/the-sequoia-rip-good-times-presentation-get-your-copy-here.

8. See, for example, Acxiom, "Data Packages," accessed March 23, 2016, http://www.acxiom.com/data-packages.

9. For instance, the proliferation of bots on the internet has reduced internet data quality and impeded price discovery in digital advertising markets. See "The Hidden Cost Bots Add to Online Ads," *Digiday*, October 28, 2013, accessed March 23, 2016, http://digiday.com/agencies/hidden-cost-bots.

10. Ronald Coase, "The Problem of Social Cost," *Journal of Law and Economics*, Vol. 3. (Oct., 1960), pp. 1-44.

11. See Adam Thierer, *Permissionless Innovation: The Continuing Case for Comprehensive Technological Freedom* (Washington, D.C.: Mercatus Center, 2014).

12. See Geneviève Bonnelye, Andrew Miniuks, and Alice Goncalves, "The Importance of Real-World Data to the Pharma Industry," PMLiVE, June 26, 2015, accessed March 23, 2016, http://www.pmlive.com/pharma_thought_leadership/the_importance_of_real-world_data_to_the_pharma_industry_740092.

13. The US Department of Energy's "Nuclear Cities Initiative" addressed this issue starting in 1998.

14. A "systemic risk entity" is a financial institution judged by the Federal Reserve to be critical to the health of the overall financial system. It is possible to imagine an analogous label for large technology and data firms.

15. The original Safe Harbor agreement was invalidated by court order in 2015. See Kelli Clark, "The EU Safe Harbor Agreement Is Dead, Here's What To Do About It," *Forbes*, October 27, 2015, accessed March 23, 2016, http://www.forbes.com/sites/riskmap/2015/10/27/the-eu-safe-harbor-agreement-is-dead-heres-what-to-do-about-it/#68d25ad71719.

16. Data sales in bankruptcy are not without precedent. See Jenn Topper, Ivan Kallick, and Jesse Brody, "Consumer Data in Bankruptcy: Saleable Asset or Liability?," *Law360*, April 10, 2015, accessed March 23, 2016, http://www.law360.com/articles/641433/consumer-data-in-bankruptcy-saleable-asset-or-liability.

17. James Manyika, Jacques Bughin, Jonathan Woetzel, Susan Lund, Kalin Stamenov, and Dhruv Dhingra, "Digital Globalization: The New Era of Global Flows," *McKinsey & Company*, February 25, 2016, accessed March 23, 2016, http://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-globalization-the-new-era-of-global-flows.

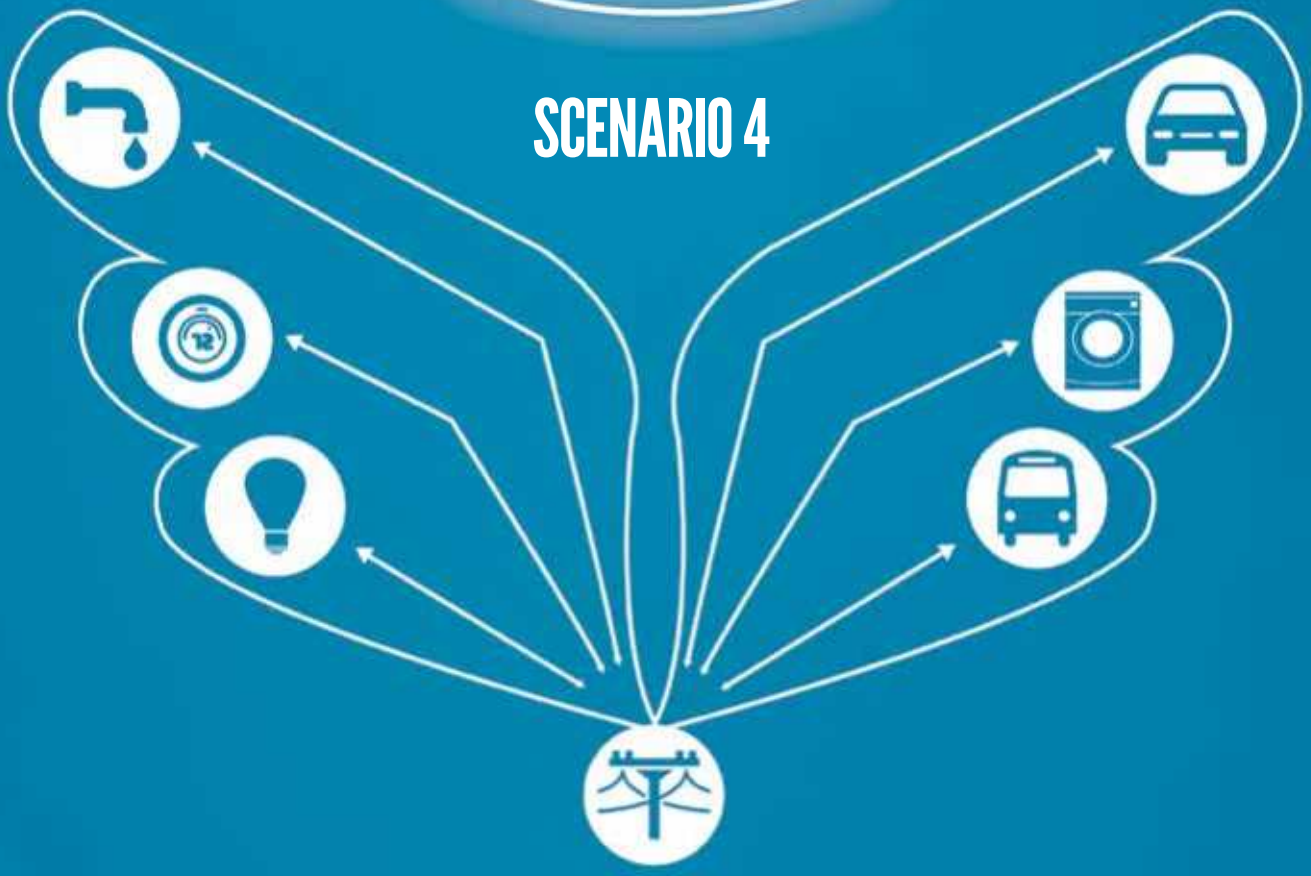
18. Much of the story of *The Godfather: Part II* (1974) is about the leader of the Corleone family trying to convert the crime syndicate from illegal to legal businesses as a way of enhancing growth and reducing risk. Digital criminals motivated principally by profit might be tempted try the same in this scenario.

19. See Laney Salisbury and Aly Sujo, *Provenance: How a Con Man and a Forger Rewrote the History of Modern Art* (New York: Penguin, 2009).

20. For the state of affairs as of 2015, see Privacy Rights Clearinghouse, "Fact Sheet 41: Data Brokers and Your Privacy," last revised December 2016, accessed March 23, 2016, https://www.privacyrights.org/content/data-brokers-and-your-privacy.

For more information on the Center for Long-Term Cybersecurity or these scenarios, please visit **cltc.berkeley.edu.**

SCENARIO 4



INTENTIONAL INTERNET OF THINGS

This is a world in which "Internet of Things" (IoT) technologies—everyday products, devices, and structures connected to the network—are integrated intentionally, boldly, and relatively smoothly into the developed world.

While the widespread adoption of IoT technologies may be predictable in 2016, the mechanism that will propel this shift is less so. In this scenario, government will intentionally drive IoT adoption to help societies combat recalcitrant large-scale problems in areas like education, the environment, public health, and personal well-being. This will be widely seen as beneficial, particularly as the technologies move quickly from being household novelties to tools for combating climate change and bolstering health. "Smart cities" will transition from hype to reality as urban areas adapt to the IoT with surprising speed. In this world, cybersecurity will fade as a separate area of interest; when digitally connected technologies are part of everyday life, their security is seen as inseparable from personal and national security. But while this world will offer fantastic benefits for public life and reinvigorate the role of governments, there will also be greater vulnerability as IoT technologies become more foundational to government functions and the collective good.

THE WORLD

In this scenario's version of 2020, the Internet of Things (IoT) has moved beyond Silicon Valley slide decks and fitness and sleep-tracking wearables to become a purposefully chosen and essential part of daily life—at least in the developed world. IoT consumer devices in 2016 are still largely seen as luxury items with limited applicability—more fun than substance. In 2020, the opposite will be true. Governments will identify huge benefits to smart-designed devices. Through acts of "positive paternalism" (intentional government action designed to improve public life), governments will deploy and implement the IoT in myriad aspects of human life.

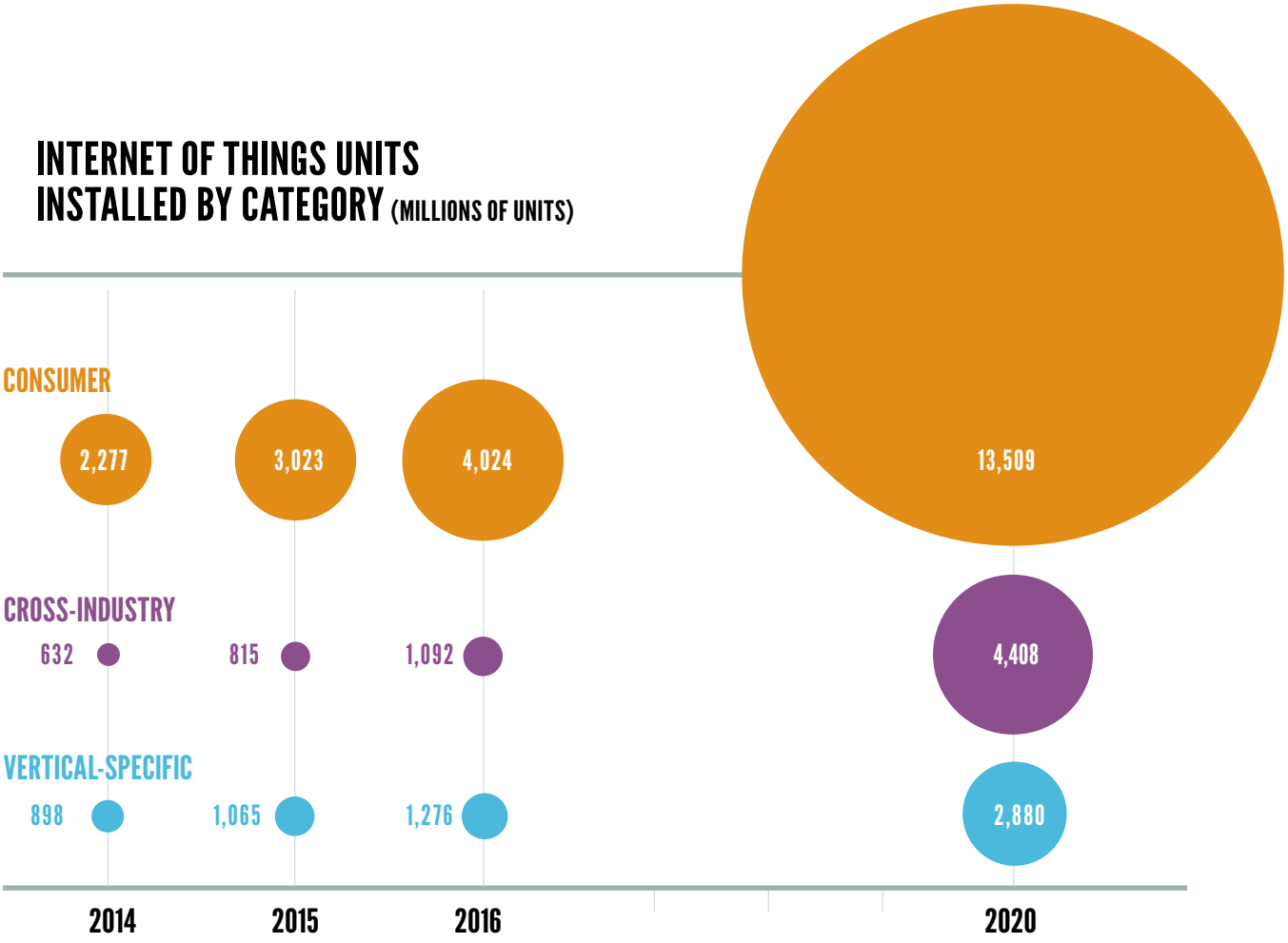
In this world, the IoT will not just mean refrigerators that automatically replace your milk when it runs out, or credit cards that vibrate every time an expenditure is charged. It will mean smartbands that diagnose health problems as they occur and dispatch medical care without human intervention. It will mean smart-metering for oil, gas, and electricity; traffic lights that automatically change based on congestion patterns; and wearable sensors—the successor to Google Glass—that help classroom teachers track whether students are paying attention. In this world, governments will be back in business as major providers of public infrastructure creating new, highly technical products that serve the public interest. The private sector will follow in kind—and a whole host of new cybersecurity vulnerabilities will develop as a result.

The driving forces behind the emergence of this "intentional IoT" are clearly visible in 2016. Embedded systems and sensors are becoming widespread. Disneyworld's MagicBand bracelets allow park visitors to pay for items, reserve rides, order food, and get personalized experiences; they also allow the park to track visitor flows and optimize the distribution of employees, food, and other services.[1] Smart-lighting networks in streets, parking lots, and malls use LEDs, sensors, and data to turn lights on and off automatically, monitor pollutants, listen for gunshots, or track traffic and even shoppers. The "Quantified Self" movement, once dismissed as a geek hobby, is demonstrating that individuals can use sensors to self-track meaningful, actionable health data about themselves.[2] On the government side, the US Department of Transportation is developing models for an internet-connected road and vehicle ecosystem—a wireless communications network that connects cars, buses, trucks, trains, traffic signals, smartphones, and other devices in order to improve safety and traffic flows and create more environment-friendly transportation options.

Through acts of "positive paternalism" (intentional government action designed to improve public life), governments will deploy and implement the IoT in myriad aspects of human life.

All the ingredients are in place. But what is not yet clear in 2016 is where the breakthroughs that will define the IoT for the next decade will emerge. Will it be large private-sector actors, pressing forward with a General Electric-type vision of an industrial internet?[3] Will it be an IoT driven forward by law enforcement and the intelligence community's desire for granular surveillance?

In this scenario, it is neither economic productivity nor national security interest, but rather a "public good" IoT that pulls ahead and dominates the landscape. This is an IoT in which governments (with private partners) drive the adoption of new technologies designed to improve



SOURCE: GARTNER: http://www.gartner.com/newsroom/id/3165317

the lives of communities, including by upgrading their critical infrastructure systems. It is this vision of the IoT that garners the most resources and the most attention—and sets many of the key technical, economic, and regulatory terms for the IoT overall.

Smart cities in high-tech, high-control places like South Korea (the city of Songdo) and the United Arab Emirates (Mazdar) will be early indicators of this shift, as they implement more expansive visions of the IoT to combat problems inherent to dense urban living. In the next several years, planners of these cities will argue openly that human behavior could and should be "managed" by IoT applications in order to more effectively deal with the social, economic, and environmental challenges of city life. Importantly, such cities will be in a position to make that argument without the negative valence regarding surveillance that accompanies similar arguments in the Western world.

The real shift toward widespread IoT adoption would happen when governments in the United States embrace this new model in a more focused manner, probably as a response to urgent public needs. For example, California governor Jerry Brown might in 2017 announce a massive state investment in IoT technologies to respond to the state's drought and water crisis. Sensors would be installed in rivers, dams, farms, groundwater, water districts, sewers, businesses, and homes, coupled with water-regulating instruments and on-demand water recycling devices, to create an IoW (Internet of Water) network that would provide precise data to the state and more effectively manage the incentives for citizens and businesses to conserve.[4] Releasing this data into the public domain would create a vibrant market for private companies to build and sell new services and devices linked to the system—assuming, of course, the state of California is willing to restrain from overregulating it.

A massive, high-profile IoT initiative like this might very well gain broad public support as a "positive paternalist" action, the benefits of which overshadow vague and hypothetical concerns about privacy. Supporters will argue that, during a severe drought that threatens California's fundamental sustainability as a society, how much water a home or business uses can no longer be considered a private matter, any more than an individual's vaccination status can be considered a private matter during a severe epidemic.

In 2016 there is substantial willingness to accept the idea of government accessing vast swaths of private data in the name of counterterrorism surveillance. In this scenario, the public will become comfortable with granting even more access in the name of public progress, in part because the benefits will be more transparent, representing the creation of a public good that people can see and experience, as opposed to preventing a public ill that by its nature is invisible.

If the California "Internet of Water" begins to generate significant reductions in water use even during its first year or two of deployment, the notion of an "intentional IoT" will have gained a major foothold inside the United States. The benefits of this shift would be almost irresistible, and similar movements toward intentional IoT would follow in the rest of the developed world. At the 2018 UN Cyber Summit in Hong Kong, international standards for the storage, transmission, and encryption of IoT data might be consolidated, as the Gates Foundation and Chan Zuckerberg Initiative announce new low-cost, global "megaband" wireless networks to facilitate further IoT adoption. In 2019, not only major sporting events but reserve military training and complicated surgery practice might be featured as visible payoffs from distributed, immersive virtual reality. By 2020, personal security sensors built into clothing and other accessories might provide real-time data to police in Los Angeles about possible violent outbursts. Simultaneous outrage and acclaim will erupt. But the "public good" arguments will generally win the day.

The public will become comfortable with granting even more access in the name of public progress, in part because the benefits will be more transparent . . .

In Europe, there will be deeper ambivalence about, and more resolved public resistance to, these developments. Europeans will see the United States solving some prickly public-good problems and will be tempted to encourage their governments to follow suit. At the same time, they will fear how these innovations undermine "traditional" ways of doing things, not least because many (most?) of these devices will be developed and sold by American companies and require the adoption of "American" principles of government management (including delegation to the private sector). One possibility is that Europe will implement new and stronger privacy protocols to enable a greater degree of comfort with these technologies, thereby slowing progress relative to other parts of the world. Would this become a new front in the economic competitiveness wars?

In cities and countries that do throw in with the new intentional IoT, public-private partnerships will flourish. For example, the Alphabet Intelligent Roads Center, the US Departments of Transportation

FROM THE FUTURE

http://www.cyberblog.com/current-post/presidents-digital-contract-with-america.html

CYBERBLOG Jon Kline, August 14, 2020 @ 8:25pm 1006 Views

Reflecting on the President's "Digital Contract with America"

+ Comment Now + Follow Comments

In this year's State of the Union address, the president proclaimed success in her "Digital Contract with America" initiative, an effort representing massive government investment and public-private partnerships focused on technology across almost all sectors of the US economy. Seven months later, the initiative has become central to her bid for reelection, even as she faces criticism that her efforts will create an unfunded mandate for years to come.

The Digital Contract with America began in January 2018, when the White House announced a series of federal programs designed to stimulate the sluggish economy by making use of Web 5.0 technology, also known as the "intentional Internet of Things" (intentional IoT). The term describes the environment of internet-connected sensors and machines embedded in our daily lives, from cars to watches, streetlights to coffee machines, and water pipes to door locks.

The initiative led to the launch of hundreds of Web 5.0 projects, in both private and public sectors, including the rollout of Drink Smart soda vending machines in New York City, the St. Louis Smart Desks program, Apple's personalized "Replicator" food machines, and Seattle's "Green Lights for Green Cars" initiative.

Majorities in the Democratic Senate and Republican House have passed a number of bills moving the country toward the administration's vision of "private partnerships and investments in technology that help us overcome some of our greatest challenges." A bipartisan group has passed 11 bills so far this year. Below are some highlights:

- The National Science Foundation is studying the possibility of tapping into the dormant computing power of internet-connected devices when they are in standby mode to create a massive Cloud Microcomputing Infrastructure, which could be used to help calculate physics problems and analyze photos and signals from space.
- The McGraw Hill EduBracelets pilot program launched in Los Angeles, Tampa, Denver, Chicago, and Philadelphia. Bracelets worn by children allow teachers to craft individualized lesson plans, and allow parents to easily keep track of their children's progress. The bracelets can also talk to toys and apps that are Common Core approved, allowing teachers to see what students are learning outside of the classroom.
- According to recently leaked documents, the CIA received funding last year to create secret government versions of IoT devices (built by shell companies) to ship to Iran and Venezuela that would nudge young people already amenable to dissent to stir political unrest.

Despite bipartisan support, some lawmakers have criticized the White House's recent decision to cut funding to other initiatives in order to fund more Web 5.0 programs. Others have argued that the program could do more. While ACLU lawyer Eric Medina praises programs like CitySensors, which provides discounted sensor kits to low-income urban families, he says "there are swaths of urban and rural America that still lack access to broadband-speed internet who cannot make use of all of these wireless services."

The latest Reuters instant poll of 300 million Americans shows the Digital Contract with America garnering a 67 percent approval rating.

and Homeland Security, and the state of Nevada might create a joint $10 billion investment over five years to upgrade all of Nevada's highways to new SmartRoad 2.0 standards—enabling smart cars to communicate directly with roads. The vast data made available from a large-scale public-private initiative like this would be open to public scrutiny at a micro level. Outputs from such a consortium might include fewer accidents, a reduction in carbon emissions, and a rise in road capacity efficiency—and all before the institutionalization of driverless cars. A tangible reduction in traffic jams and measurable improvements in commuting time could secure public approval for the intentional IoT in other domains.

Such successes would become the roots of a broad social movement rising around the IoT. For instance, a coalition of engineers, policymakers, and social activists might come together to promote the "Intentional by Design" movement. This movement would call for IoT technologies to move beyond last decade's "neutral platform" notion and onto a much more positive, activist concept of IoT build-out. The difference? The new platforms would contain specific and explicit "intent" to help solve societal issues.

With public support and commercial and government commitments in place, new investments in underlying technologies that could be quickly deployed will spawn a positive feedback loop where (at least for a time) applications would improve at an increasing rate. Low-cost sensors and mobile devices will see improved performance as the hardware foundation for the intentional IoT expands. Gains in available wireless spectrum and the adoption of new updated Wi-Fi and Bluetooth standards will make it even easier and cheaper to deploy wireless devices. The growth of distributed computing will help reduce the overhead of doing massive processing on a central server, allowing ad hoc networks of devices to engage in de facto "mesh" super-computing. Advances in and greater availability of data tools will allow engineers and data scientists to create "brilliant" devices that not only respond to their environments but reconfigure themselves within adaptive networks. The IoT might even become a driving force behind new developments in encryption to secure the transmission of data between low-power, inexpensive distributed devices.

New platforms would contain specific and explicit "intent" to help solve societal issues.

This virtuous circle will continue for some time, and as it does, the scope and impact of the IoT will expand apace. Intentional IoT systems will be deployed in transportation, environmental, educational, health, military, and safety domains. The bolder the deployment strategies, the more compelling the results. Imagine a 2020 finding that vehicle accidents among people owning IoT cars have decreased by 36 percent, or that following the implementation of IoT Star[5] refrigerators, the percentage of overweight Americans has stabilized (or even fallen a few percent). Or imagine that graduation rates for the first high-school class using IoT education systems increased by 7 percent. These developments would plausibly create a (much-needed) boost to overall economic growth in the United States. If US GDP were to jump 4 percent by the end of the decade, tied at least in part to IoT deployments, could the intentional IoT be seen as doing what the Federal Reserve and other central banks could not do—provide the antidote to a decade of secular stagnation?

FROM THE FUTURE

Sign up today for your

PG&E HOME SENSOR NETWORK AUDIT!

We are pleased to inform you about a new package of services that will soon be available to PG&E customers.

Through our new Home Network Security Audit, you will gain the confidence of knowing that your connected devices are fully secure.

Call us today, and within one week, a certified network specialist will visit your home and:

- Conduct tests to ensure that your home network is secure and up-to-date, and that your home appliances are properly connected to the internet.
- Install any security patches necessary to bring your system to the highest levels of security.
- Share with you data about your usage and other packages that may be available.

Don't wait! Call to sign up for your Home Sensor Network Audit today!

OUTCOMES

The intentional IoT in this scenario will for many fulfil the promise of new technologies. After all, this vision aligns with what idealists of the early internet era (indeed, even of the Homebrew Computer Club era) believed digital technologies were supposed to achieve for people and societies. The winning argument might be simply that "wicked problems"[6] like climate change and public health crises are too important—and have proved too hard—to solve by other means. These critical public-good "use cases" will drive and justify the investment (and risk) in the ambitious deployment of the intentional IoT. In this world, a large-scale IoT will have significant effects on nearly every aspect of people's daily lives.

There will be enough delightful and meaningful experiences with the new IoT, from the profound to the mundane, to keep most people optimistic. Seamless personalized services foreshadowed at places like Disneyworld will become normalized and expected in many areas of life, including (to a surprising degree) in government services and healthcare. Devices will automatically send payments to other devices. Interpreting parking signs will become a thing of the past, as cars will know exactly how much to pay. Starbucks will create the Select SmartCup, a special IoT-enabled reusable cup that lets customers skip the line and head for a special machine that automatically creates a custom drink to their distinct taste (and automatically pays for it, of course).

FROM THE FUTURE

Starbucks' new "Select SmartCup" allows you to skip the line and go straight to a robot-barista that automatically creates a custom drink based on your preferences–and deducts payment from the cup itself.

Behind these headline gee-whiz stories will lie a deeper and more profound shift in social attitudes toward digital technologies. The ambivalence that in 2016 many people feel about the digital revolution will fade into the background (again) with this new burst of benefits that puts the IoT front and center in daily life. As happened with the World Wide Web during its first few "real" years, the IoT will become the focal point of public conversation. Academics will analyze and compare how countries use the IoT, shifting the comparison away from welfare-based vs. market-based forms of capitalism toward segments based on breadth and depth of IoT applications. Leading public intellectuals and political theorists will examine other dimensions of intentional IoT use, such as public vs. private implementations; whether these technologies generate greater benefits for labor or capital; and how much they cater to individual, communal, or societal problems. These will be seen not as speculative or marginal discussions, but rather as cutting-edge debates about a new technology horizon.

As always with digital technology, the most immediate and vehement counterarguments will come from privacy advocates raising the alarm about potential harms. But for the vast majority of people, the IoT's benefits will outweigh concerns about mostly hypothetical risks. The American middle class in particular will aspire to use IoT technologies to "regain control" over health, family, work, and education. Much in the way that smartphone users today are willing to expose geolocation and identity data for the convenience of using top apps, in 2020 middle-class users will be willing to trade away even more information about themselves for an IoT-enabled lifestyle. For most, this choice will not even be perceived as a tradeoff.

At the same time, aspirations for IoT technology will not quite be matched by reality. New types of inequality will arise quickly and with possibly savage consequences in this world. The quality of services will differ dramatically for people unable to access the IoT compared to those who do have access. While the percentage of Americans not meaningfully connected to IoT systems would likely fall below 10 percent by 2020, that unconnected population (mostly those living below the poverty line and in rural areas) might see the quality of their public services corrode even further. Insurance costs will rise for people who are unable to buy personalized health devices, retrofit their homes with IoT appliances, or access new smart cars. People living in areas that lack IoT sensor deployment will suffer as cities and states increasingly adopt data-driven investment and maintenance practices (foreshadowed in 2014 by problems with a crowd-sourced pothole detection app in Boston).[7] Some of the disconnected will lose the ability to find fruitful work in the IoT-enabled economy: driverless cars, automated machinery lines, and electronic personal assistants will leave lower classes competing for increasingly scarce service jobs.[8]

The quality of services will differ dramatically for people unable to access the IoT compared to those who do have access.

These labor market effects were coming in any event, but in this world, the IoT will become a convenient locus to place the blame. Many groups that initially opposed the intentional IoT because of surveillance concerns would likely shift their focus toward measures that aim to alleviate new types of inequalities, particularly those around jobs.

Other industries that will be deeply affected by this shift, such as healthcare and education, will face a different problem: how to reap the benefits of the IoT without giving away the most important parts of their value chain and thus ceding market power to IoT companies. In 2016, some large healthcare and hospital firms are already developing their own IT systems, patient apps, etc., precisely to avoid tech company monopolies. By 2020, retail companies and large networks of schools may be doing the same. The smaller fish in these ponds will face more difficulties in matching these parallel IoT initiatives. For them, the choice is most stark: either lose a critical point of control in their business models or drop out of the race for the IoT altogether.

The Internet of Things will also become a part of consumer-dependent industries in new and innovative ways. Consider clinical drug trials: in 2016, most participants find their way to trials by word-of-mouth and lengthy screening processes. In 2020, the IoT for Clinical Trials will replace these informal and highly inefficient networks. Patients will be contacted about their eligibility for trials through automatic electronic screening systems and will be able to participate remotely using data already being captured through their personalized health IoT systems. Pharma companies could see a huge burst in new therapeutics being approved as a result.

The shift in attitudes toward the intentional IoT would be a boon for technology-first sectors that focus on automation and robotics. In fact, robots could come to be seen as the "next big step." Particularly in areas such as transportation and logistics, it might become increasingly legitimate to argue that "the more autonomous the robot, the better the outcome for humans." The CEO of Toyota might quote Abraham Lincoln in a keynote speech at the 2020 "Internet of Things World Conference" (which would have by now replaced RSA as Silicon Valley's preeminent information security conference), referring to the IoR (Internet of Robots) as expressing "the better angels of our nature."[9] Today's big internet companies—the Googles and Apples of the world—will increasingly focus on developing devices that have physical actuators, whether or not they label these as robots.

Particularly in areas such as transportation and logistics, it might become increasingly legitimate to argue that "the more autonomous the robot, the better the outcome for humans."

The ICT4D community (information and communications technologies for development—a social movement aimed at bridging the gap between technology and community development) would likely come to see the intentional IoT as a central new part of its approach, though, as in the past, there will be a variegated mix of successes and failures.[10] ICT4D projects might well experiment with the use of blockchain technology for the transfer of IoT data, as foreshadowed by current IBM and Samsung projects.[11] This would allow devices to communicate directly and reliably with one another in a decentralized system, reducing overhead and lessening the need to build large internet infrastructures in geographies that do not already have them.

In this scenario, the intentional IoT will become a critical policy lever for governments. The main policy debate will be not about whether we should use the intentional IoT to address governance and

policy challenges. Rather, it will be about how the intentional IoT should be implemented, and whose intentions will be programmed into the system. The same debates that have swirled around digital technologies for 20 years—who makes design decisions and how laws and regulation should interact with engineering and design—will find their way into intentional IoT debates. Given the public interest in speeding the adoption of IoT technologies, governments will feel pressure to act much more nimbly than they have in decades past.

Federal, state, and municipal governments alike will see the IoT as a way to break logjams and get more done. A diversity of new and ambitious initiatives will result: in some cases, multiple actors will compete in the same domain; in others, stretch initiatives will fail to live up to their potential (think Boston's "Big IoT Dig" starting in 2019). And in still others, governments may deploy technologies before they are ready. In the United States, new investments in the IoT energy grid will bring the country significantly closer to a national smart grid. In other domains, such as immigration, approaches and results will be more controversial. Will there be a real employer verification system? A virtual wall? Smart identity cards? IoT technologies will make all of these feasible but not any easier to agree upon.

As a result of these new IoT-enabled problem-solving approaches and efficiencies, the perception that "government cannot get anything done" will begin to drop out of public rhetoric.

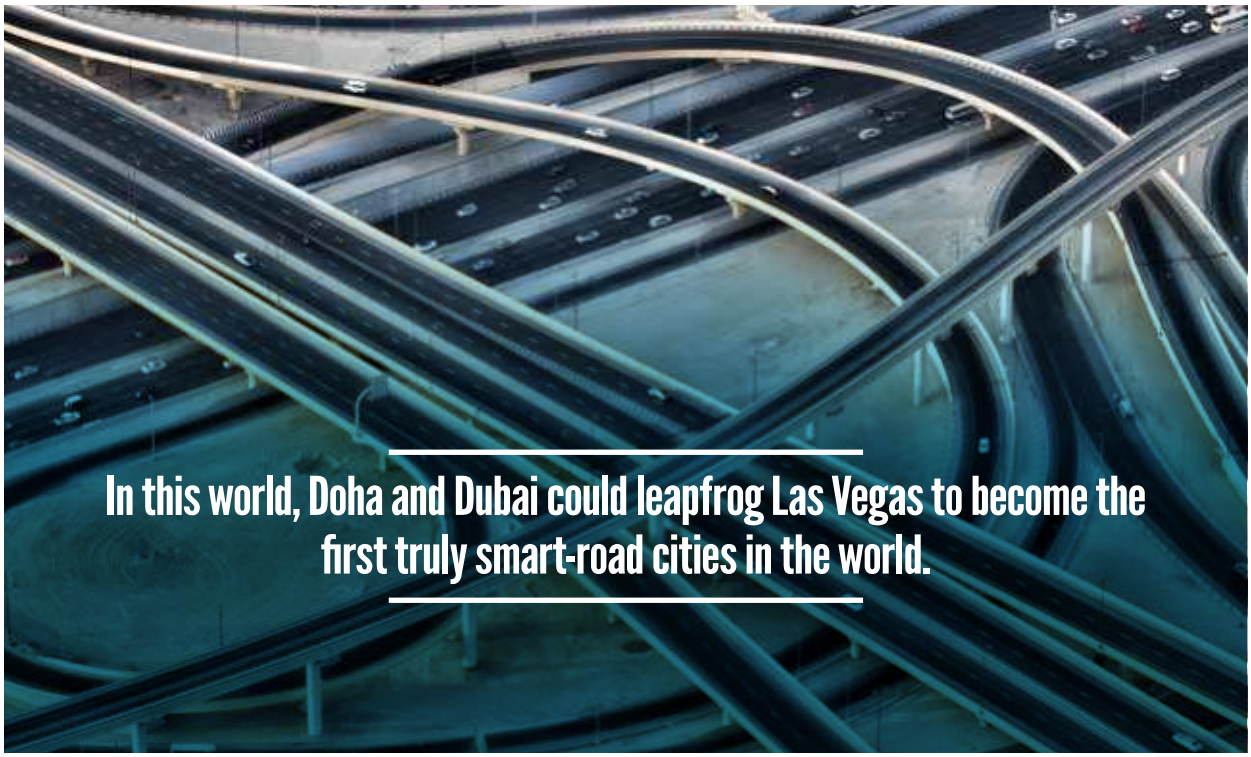
The implications for citizens' day-to-day lives could be sweeping, but perhaps the most significant impact will be on government itself. As a result of these new IoT-enabled problem-solving approaches and efficiencies, the perception that "government cannot get anything done" will begin to drop out of public rhetoric. The public will reap the benefits of IoT systems, and even be willing to pay taxes(!) to expand their impact. For the vast majority of public systems, this is great news. For systems that have grown to be dependent on the "fuzzy edges"—employment of undocumented immigrants in agriculture, for instance—the effects will be more mixed, with significant unforeseen consequences. When government fails to take enforcement action, the reason will no longer be incompetence. It will be, or at least be understood as, a purposeful choice.

Will the IoT be a global network? Probably not, as China's "Great Firewall" would most likely be extended to IoT devices, made and programmed by Chinese companies and mostly inoperable with Western IoT devices. The Chinese government will see massive value in the intentional IoT to improve citizens' lives and monitor the actions of potential dissidents—but it will be wary of American IoT devices and software that might be used to empower dissidents to connect and communicate with one another or to "monitor" Chinese economics and politics from abroad. Concerns about "backdoors" and hardware built abroad with deliberately engineered defects will limit the readiness of autocracies in the developing world to import large numbers of foreign-made devices. The United States will share these concerns, and would probably become equally wary of imports. This would be another driving force pressing toward re-nationalization of at least some technology production and the possible emergence of nationally based, conflicting standards for device

communication and interoperability. One can imagine that the Trans-Pacific Partnership trade agreement would have to add an IoT codicil by 2020.

For smaller countries not able to access economies of scale at the level of China or the United States, the choice will be framed as one between economic and monetary spheres of influence: join the US IoT, the Chinese IoT, or try to go it alone? Countries like Singapore that are already oriented toward a strong paternalistic state would find they also have an interest in using the intentional IoT for purposes beyond monitoring and surveillance, to nudge behaviors in ways they believe are positive for their societies. Surveillance (somewhat ironically) might become less noxious, as the mix between empowering state control of individuals to aid state power and improving the economic and social conditions of people tilts more toward the latter. Would countries like Qatar or the UAE become leaders in developing and fine-tuning this mix, deploying sensors in every roadway and car? In this world, Doha and Dubai could leapfrog Las Vegas to become the first truly smart-road cities in the world.

This combination of fascination with potential gains and anxiety about "national" technologies in the context of the IoT will also emerge as a transatlantic issue. Americans will expect Europeans to be as enthusiastic as they are about the new technologies; everyone has smartphones, after all, and do European consumers really miss Nokia? Given that Europeans are believed to be more trusting of "the state" than Americans, there is the possibility that adopting the IoT for the public good will be a very attractive argument in some countries. But many Europeans will be ambivalent and resistant, given privacy concerns and the changing role of government. This could be particularly important if American firms get aggressive about promoting their products and run roughshod over concerns (justified or not) about "too much data flowing back across the Atlantic into Silicon Valley."



In this world, Doha and Dubai could leapfrog Las Vegas to become the first truly smart-road cities in the world.

Cybersecurity of Things

In this intentional IoT world of 2020, there will no longer be an "internet and society" discussion; there will simply be a "society" discussion, as the internet fades into the ubiquitous background. And because digital technology is now present in almost every domain as part of the intentional IoT infrastructure, the term "cybersecurity" will feel dated. Cybersecurity will just be "security," seen through the lens of traditional domains. IoT devices in the home will be in the realm of personal security; smart infrastructure and government-run systems will be part of national security; sensors and devices to deal with climate and energy will be a dimension of environmental security; and so on.

Technical expertise will be critical to all these domains, but the "cybersecurity specialist" model of years past will give way to a wider suite of skills that technical experts need to get systems running and keep them in working order. Preventing attacks and creating defenses will be as important as domain expertise, whether in the education, financial, or healthcare sector. The technician who visits your home to repair a washing machine or the airline mechanic who steps onto your plane in 2020 will have what in 2016 would have been considered pretty significant "cybersecurity" training. Basic device security might become a core part of the standard university or professional school curriculum.

Encryption will increasingly be built into most intentional IoT systems components by default. One of the challenges will be pushing out updates and patches on what might be a very frequent schedule, at the scale of billions of devices. With faster product development cycles, people and organizations will have to contend with many rapidly outdated IoT devices, as well as the burden of legacy devices that are still operational but no longer receiving updates, or that are no longer technically capable of implementing new encryption or other security systems. Non-digital companies—from Lenscrafters to pipe manufacturers—will suddenly be tasked with putting sensors into their products; since such companies will have limited experience with computer security, their products are particularly likely to be vulnerable. The rapid rush to deploy the IoT will compound this problem, leading to security sloppiness that will be very hard to audit, much less clean up.

Preventing attacks and creating defenses will be as important as domain expertise, whether in the education, financial, or healthcare sector.

High-end criminals and ambitious terrorists will focus their attention on the most serious cyber-physical targets, such as critical infrastructure. Terrorists in particular will seek to undermine the growing confidence in Western governments created by the intentional IoT; ISIS and similar groups or their successors will see this confidence as an existential threat to their message and the political order they are trying to create. Plausibly, the IoT would replace the airplane as the nexus of terrorist attentions.

To access key targets, attackers will continue to seek vulnerabilities in outdated systems as an entry mechanism into more sensitive attack points, as they often do in 2016. But there will be more such "unaudited" interdependencies in 2020. To attack Google's digital suite of service providers, a state actor might jump from traffic lights to the operating system of vehicles to the servers that manage traffic databases, and from there to Google's robot operating systems.

Large state actors will similarly try very hard to penetrate one another's core systems (much as they do today). But the stakes will be much higher in the 2020 intentional IoT world, because the possibility for a truly catastrophic attack will be significantly higher. These pressures will likely create an anxious state of deterrence equilibrium between world powers (the United States, China, and Russia). "The threat that leaves something to chance" had to be engineered into the nuclear deterrence world of the second half of the 20th century to enhance stability, but it will naturally be part of the IoT world due to the layers of complexity in relevant systems. Whether this comes to be perceived as a new "mutually assured destruction" equilibrium that creates a kind of strategic stability, or a very tense "first-strike advantage" environment that could be highly unstable, this dynamic could become one of the most important uncertainties that the major power states will confront. For smaller states, the choice may be reduced to picking sides by assessing security risk as much as—or more than—traditional political leanings. If China is seen as providing better IoT security than the United States, will Turkey or India throw in their lots with China instead?

Despite states' best effort to engineer against them, attacks and failures will still occur, sometimes at a large scale. Imagine that the smart traffic control system of Mumbai is attacked, causing cars to drive into one another and killing 1,000 passengers in minutes. Or a chemical factory's systems could be hacked, contaminating water sources for several towns in France. Would these be turning points? In this world, probably not, as long as single failures do not cascade into systemic failures. As with accidents in socio-technical systems of the past— plane crashes, E. coli outbreaks, or defective airbags—the media will pay close attention, but most people will continue to use these systems because they do not see an alternative. Failures that occur with the intentional IoT are likely to seem similar. Investigations will occur, new rules will be put into place, and consumers will be made aware of preventative measures they can take—but the overall system will march on.

For lower-level criminals unable to infiltrate the most highly protected systems, new types of attacks might focus on intentional IoT algorithms. Micro-attacks will try to alter such algorithms in small, seemingly undetectable ways. These changes will often be invisible until the results—which can take time to manifest—become widely visible. Consider a system that monitors the drinking habits of individuals genetically predisposed toward alcoholism. If an attacker could manipulate the algorithm so that a few more drops of alcohol can be consumed each day, the attack would likely go unnoticed until the individual lapsed into alcoholism. Or imagine a slight retuning of a million engines in gas vehicles resulting in an almost undetectable increase in gas consumption, which would in turn raise oil prices by one penny per barrel around the world. At scale, these kinds of manipulations could become the modern version of the mailbox "lottery scam" for financially motivated criminals.

But it might not only be criminals who find this sort of attack interesting. Analogous manipulations may come from those who are disadvantaged by the growing IoT-enabled sense of inequality. "Domestic" disruptors and terror groups will try to bring systems down in dramatic fashion in order to call attention to their dissatisfactions. Other attacks might come from within the corporate sphere itself; someone who controls a counterfeit statin drug factory might want to manipulate eating and exercise behaviors in an unhealthy direction so as to spur demand for their (counterfeit) product.

FROM THE FUTURE

http://www.cyberwire.com/business-news/dragon-drone-products.html

CyberWIRE

Business News: Comcast Acknowledges Problems with Smart Locks in "Dragon Drone" Products

EMILY LOPEZ
August 14, 2020
CyberWire

Comcast issued a press release on Thursday regarding recently exposed problems with the wireless door locks used in its "Dragon Drone" Smart Everywhere products.

Dragon Drones are autonomous drones that parents can use to monitor their children. Originally released as quadcopters fitted with a camera and GPS, more recent versions of the product have been shaped to look like a variety of animals, including dragons, birds, butterflies, and dinosaurs.

Many children consider Dragon Drones to be like pets, as they can interact with the flying devices. In addition to providing traditional parental monitoring services, Dragon Drones can respond to and interact with children, encouraging them to stay physically active, play educational games, and promote cooperative play.

"I love our Dragon Drone," says Maria Abbot of Arlington, Virginia. "It picks up my kids after school, walks them to the park for soccer practice, and then walks them home. It only goes to locations that we've approved, and if the kids stray outside of that, the Drone will encourage them back while sending us an alert."

But Dragon Drones are not without their flaws. Last week, researchers at the University of Virginia identified a security issue with the software that links the Dragon Drone and a home's locks. This feature is intended to unlock a house door when the owner's Dragon Drone approaches, allowing it (and the accompanying children) to go in and out of the house without the worry of a key fob.

The researchers showed that the locks, which are produced by Chinese manufacturer Lenovo, are easily accessible over the internet. "Using the Drone's internet connection, a hacker can send enough requests to overload the lock so that it can no longer talk with key fobs, phones, or ID bracelets, which opens the locks by default," says home security expert Jules Brennen. "This makes the locks vulnerable to a distributed denial of service attack."

Approximately three million of Comcast's 15 million Smart Everywhere subscribers use these locks and have a Dragon Drone. "We are working with our partners to find a solution and will be releasing a software patch as soon as possible," Comcast announced in a written statement.

This is not the first Lenovo product that has come under scrutiny. Last year, the company's Smart Bracelets lost connectivity with other wireless devices for weeks after a software update. Some experts point to China's non-acceptance of the 2018 IEEE IoT standard as a primary cause.

"By not using the same wireless standards, it has become hard for Chinese companies to create first-rate wireless products for much of the Western world," says Garrett Yu, professor of computer science at the University of Colorado. "By the same token, it makes it much more difficult for Western countries to export wireless devices to China."

Comcast stock ended the day down almost 5 percent yesterday, closing at 145.24. Competitor Time Warner Charter closed at 164.12, down about 1 percent.

Attacks will also focus on new targets whose "expected" behaviors are not yet fully understood.[12] As machines get incrementally better at imitating human judgment, this will enable hackers to target attacks at individuals by working around the edges of what machines can and cannot do. Take what some call the "Internet of Money," created by the many devices with access to individual financial information. The refrigerator that orders your milk has your credit card information, and so do enough other IoT devices that most people will not actually know where their payment data is stored. If a large number of these devices were attacked at scale for tiny amounts, the financial gains could be significant. Information collected by IoT devices on the body could also be a key vulnerability. Would hackers use changes in Fitbit data to predict pregnancy or mental disorders in particular individuals, and threaten to disclose such information to prospective employers unless a bounty is paid? The possibilities for IoT ransomware would expand apace.

. . . the stakes will be much higher in the 2020 intentional IoT world, because the possibility for a truly catastrophic attack will be significantly higher.

The public will demand a nearly unachievable level of coordination among various partners in the sprawling IoT ecosystem in a call to improve overall security. Protecting the integrity of one's home by keeping device software up to date will require partnership among a large number of players. Updating software would probably continue to be the individual's responsibility in most cases, but companies providing home services (such as utility companies) would also be responsible for (and see a commercial opportunity in) making sure the technology is installed and updated. There will be many gray areas that allow problems to slip through the cracks. For instance, some people will believe that it is the water company's responsibility to inform residents if a leak is detected in the house, but others will contend that individual residents are responsible, given they have real-time access to water usage data.

At a national level, governments will be focused on the now much larger task of protecting societal-level intentional IoT systems, particularly critical infrastructure, including smart roads, dams, and power grids (although there will still be strident debate about what constitutes "critical" infrastructure). Maintaining the security of the IoT's "supporting" infrastructure—wireless spectrum, materials, and supply chains—will be critically important in this world, both for national security and for business and industry security. For example, systems might be built to block, jam, or spoof wireless communications. These can be used offensively (e.g., jamming communications between autonomous vehicles) or defensively (e.g., a building with walls that block interfering wireless signals, creating a safe wireless networking environment inside).

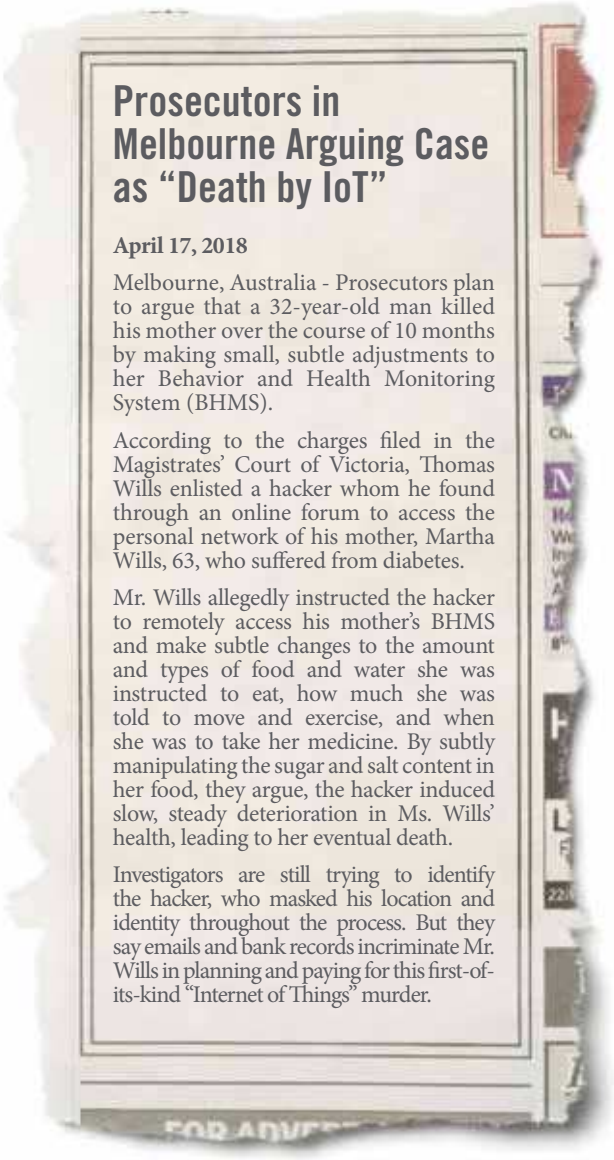
Given the risks, states might also ratchet up penalties for IoT hacking. Will Israel develop the IoT Defense Forces, a new military or law enforcement division designed to "protect the cyber-homeland"? More mundane moves—such as governments requiring adherence to particular system designs to "harden" the nation's IoT systems, or state-approved "Trusted Platform Modules"—are likely, but will always come under pressure from the pro-innovation mindset that reigns in this world. What was already a large and unwieldy state cybersecurity agenda in 2016 will expand exponentially.

Governments will continue to invest in offensive capabilities, developing ways to use the intentional IoT subversively to achieve political-military and foreign economic policy ends. As is true in 2016, the line between criminal capabilities and offensive national capabilities will be difficult to define. If criminals can move prices through small market manipulations, then surely governments and militaries could do more—for example, inducing widespread water or fuel price fluctuations. The temptation to engage in increased surveillance—through televisions, refrigerators, smart meters, and devices on the body—will also be too strong for some to resist. Fights like those between Apple and the US Department of Justice over device security are likely to get even more contentious in the IoT space.[13]

Maintaining the security of the IoT's "supporting" infrastructure will be critically important . . .

Perhaps the greatest risk lies precisely with the greatest benefits: as communities get more networked, they will also grow more vulnerable. While smart cities and smart grids will be marketed as improving societal resilience, in another sense they may actually impede it. As communities become over-reliant on IoT technologies, they will struggle to manage even the smallest disruptions to those technologies. Ironically, then, a set of technology changes primarily driven by the state and reinvigorating its role in public life could ultimately make the state weaker and more vulnerable, all because that public life will be too dependent on IoT systems. The security stakes will go up appreciably, and it will feel like it happened while no one was watching.

FROM THE FUTURE



Prosecutors in Melbourne Arguing Case as "Death by IoT"

April 17, 2018

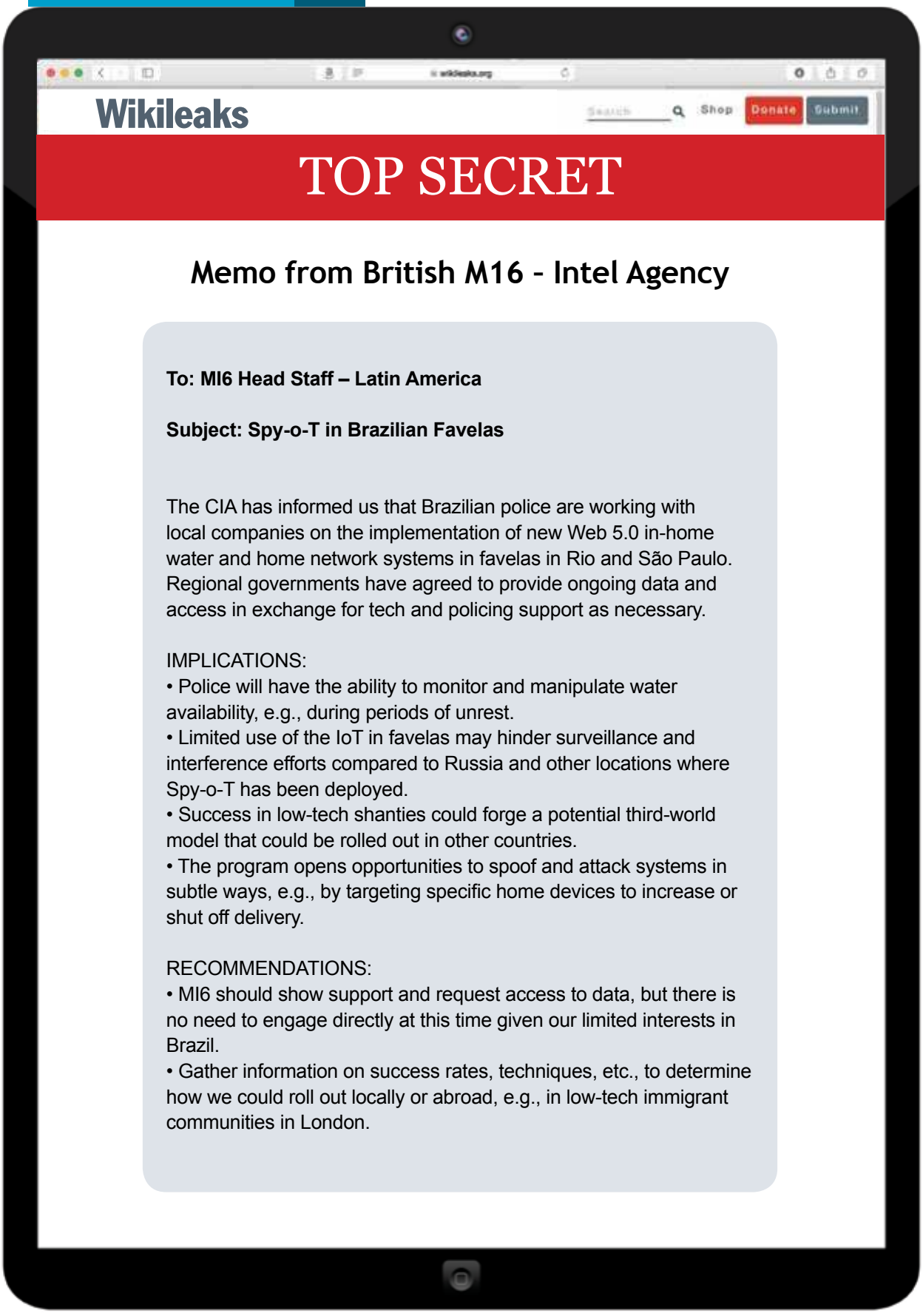
Melbourne, Australia - Prosecutors plan to argue that a 32-year-old man killed his mother over the course of 10 months by making small, subtle adjustments to her Behavior and Health Monitoring System (BHMS).

According to the charges filed in the Magistrates' Court of Victoria, Thomas Wills enlisted a hacker whom he found through an online forum to access the personal network of his mother, Martha Wills, 63, who suffered from diabetes.

Mr. Wills allegedly instructed the hacker to remotely access his mother's BHMS and make subtle changes to the amount and types of food and water she was instructed to eat, how much she was told to move and exercise, and when she was to take her medicine. By subtly manipulating the sugar and salt content in her food, they argue, the hacker induced slow, steady deterioration in Ms. Wills' health, leading to her eventual death.

Investigators are still trying to identify the hacker, who masked his location and identity throughout the process. But they say emails and bank records incriminate Mr. Wills in planning and paying for this first-of-its-kind "Internet of Things" murder.

FROM THE FUTURE



Memo from British M16 - Intel Agency

To: MI6 Head Staff – Latin America

Subject: Spy-o-T in Brazilian Favelas

The CIA has informed us that Brazilian police are working with local companies on the implementation of new Web 5.0 in-home water and home network systems in favelas in Rio and São Paulo. Regional governments have agreed to provide ongoing data and access in exchange for tech and policing support as necessary.

IMPLICATIONS:
• Police will have the ability to monitor and manipulate water availability, e.g., during periods of unrest.
• Limited use of the IoT in favelas may hinder surveillance and interference efforts compared to Russia and other locations where Spy-o-T has been deployed.
• Success in low-tech shanties could forge a potential third-world model that could be rolled out in other countries.
• The program opens opportunities to spoof and attack systems in subtle ways, e.g., by targeting specific home devices to increase or shut off delivery.

RECOMMENDATIONS:
• MI6 should show support and request access to data, but there is no need to engage directly at this time given our limited interests in Brazil.
• Gather information on success rates, techniques, etc., to determine how we could roll out locally or abroad, e.g., in low-tech immigrant communities in London.

THE WAY FORWARD

This is a world in which the Internet of Things shifts from aspirational to operational. Driven by governments newly able to resolve weaknesses in public service delivery, "smart" connected devices will appear in almost all facets of human life. IoT devices will create great opportunities to improve lives and service delivery, but these will be accompanied by new challenges and risks for users, operators, and innovators.

In this world, the public will not view IoT failures through the specific lens of "cybersecurity." Rather, they will be seen simply as failures of an individual socio-technical system, or, often, the result of human error (such as when a person fails to update his/her software). Even where the technology is shown to be at fault and surprisingly vulnerable, intentional IoT ecosystems will still be seen on balance as beneficial to humanity. People will continue using connected devices, even as the stakes of security and vulnerability mount.

In this scenario, the cybersecurity research community will wish that in 2016 it had been working on:

IOT REGULATION

How the IoT should be defined, and how it should be regulated in particular sectors (including government vs. private sector)

CYBERCRIME

How cybercriminals will change their activity if the IoT becomes the principal center of value creation in many industrial, economic, and government processes

SECURITY

How to build extremely high levels of security into the IoT system, and to foresee the type of social engineering or other attacks that will arise in this system. For instance, is there a parallel to phishing in the IoT space?

ALGORITHMS

Algorithms for managing the complexity of IoT-produced data at scale, and mechanisms for processing that data not only in narrow sectors, but across all of public life

KEEPING UP

How to keep the above-mentioned research at pace with technological innovation and the increasing levels of complexity within interconnected systems

SCENARIO 4 FOOTNOTES

1. "What Is a MagicBand?" Walt Disney World Resort, accessed March 24, 2016, https://disneyworld.disney.go.com/faq/bands-cards/understanding-magic-band.
2. The Quantified Self market is expected to grow to $5 billion by 2016. Keith Wagstaff, "Data Overload: Is the 'Quantified Self' Really the Future?" NBC News, August 30, 2014, accessed March 24, 2016, http://www.nbcnews.com/tech/innovation/data-overload-quantified-self-really-future-n189596.
3. See "U.S. Department of Transportation Announces Up to $42 Million in Next Generation Connected Vehicle Technologies," *Intelligent Transportation Systems*, October 27, 2015, accessed March 24, 2016, http://www.its.dot.gov/press/2015/ngv_tech_announcement.htm.
4. GE has argued that the internet will become instrumental to industrial processes and "deliver new efficiency gains, accelerating productivity growth the way that the Industrial Revolution and the Internet Revolution did." Peter C. Evans and Marco Annunziata, "Industrial Internet: Pushing the Boundaries of Minds and Machines," General Electric, November 26, 2012, accessed March 24, 2016, http://www.ge.com/docs/chapters/Industrial_Internet.pdf.
5. "Smart meters" for more efficient electricity delivery are already available to some California consumers. "SmartMeter™—See Your Power," Pacific Gas and Electric Company, accessed March 24, 2016, http://www.pge.com/en/myhome/customerservice/smartmeter/index.page?WT.mc_id=Vanity_smartmeter.
6. Ideally, anyone can participate in a neutral platform, irrespective of his or her ideology or position. Neutral platforms have been labeled a myth by some who believe that technology companies are only selectively neutral. Christopher Zara, "GoFundMe, Officer Wilson, Daniel Holtzclaw, and the Myth of 'Neutral' Technology Platforms," *International Business Times*, September 05, 2014, accessed March 24, 2016, http://www.ibtimes.com/gofundme-officer-wilson-daniel-holtzclaw-myth-neutral-technology-platforms-1679990.
7. EnergyStar is an existing government program that labels private appliances like refrigerators as being energy efficient. A similar "IoT-Star" program could identify IoT appliances that serve the public good—for example, refrigerators that help obese Americans track and reduce their food intake.
8. Daniel Terdiman, "Homebrew Computer Club Reunion Lights Up Silicon Valley," CNET, November 11, 2013, accessed March 24, 2016, http://www.cnet.com/news/homebrew-computer-club-reunion-lights-up-silicon-valley.
9. Wicked problems are those resistant to resolution. C. West Churchman, "Wicked Problems," *Management Science 14*, no. 4 (1967).
10. See www.streetbump.org, accessed March 25, 2016. As of 2014, the app had only a handful of regular users, and Boston was struggling to keep up with filling holes that were identified. Alice Holbrook, "Boston's Pothole App Faces Final Speed Bumps," Boston.com, July 14, 2014, accessed March 24, 2016, http://www.boston.com/cars/news-and-reviews/2014/07/14/boston-pothole-app-faces-final-speed-bumps/9uLo8dUcjn2L3zlGrAbruL/pictures.html - slide-1.
11. See Steven Pinker, *The Better Angels of Our Nature: Why Violence Has Declined* (New York: Viking, 2011).
12. For more background on ICT4D, see "Information and Communication Technologies for Development," ICT4D, accessed March 24, 2016, http://www.ict4dc.org/.
13. Blockchain uses a universal digital ledger, underlying cryptocurrencies like Bitcoin, that records transactions in a decentralized fashion so as to harden itself against security breaches. See Stacey Higginbotham, "Check Out IBM's Proposal for an Internet of Things Architecture Using Bitcoin's Block Chain Tech," Gigaom, September 9, 2014, accessed March 24, 2016, https://gigaom.com/2014/09/09/check-out-ibms-proposal-for-an-internet-of-things-architecture-using-bitcoins-block-chain-tech; Colin Barker, "Is Blockchain the Key to the Internet of Things? IBM and Samsung Think It Might Just Be," ZDNet, January 21, 2015, accessed March 24, 2016, http://www.zdnet.com/article/is-blockchain-the-key-to-the-internet-of-things-ibm-and-samsung-think-it-might-just-be; and Arvind Krishna and IBMVoice, "How Blockchain Provides the Underpinnings of Bitcoin," *Forbes*, October 8, 2015, accessed March 24, 2016, http://www.forbes.com/sites/ibm/2015/10/08/how-blockchain-provides-the-underpinnings-of-bitcoin/ - 36198ef02050.
14. See Farhad Manjoo, "The Apple Case Will Grope Its Way Into Your Future," *The New York Times*, February 24, 2016, accessed March 24, 2016, http://www.nytimes.com/2016/02/25/technology/personaltech/the-apple-case-will-grope-its-way-into-your-future.html?emc=edit_tnt_20160225.

For more information on the Center for Long-Term Cybersecurity or these scenarios, please visit **cltc.berkeley.edu.**

SCENARIO 5

SENSORIUM (INTERNET OF EMOTION)

This is a world in which high-fidelity, ubiquitous sensors and advanced data analytics make it possible to gain deep insight into human emotional experiences, a kind of insight that until roughly 2020 will be extremely difficult for humans to assess at scale.

More familiar types of data that in 2016 are expected to make a big difference—granular traffic data or data gathered from smart homes—turn out to be mildly interesting but not transformative. The greatest gains, commercial and otherwise, will instead be made through technology that measures how people feel: how mind states and memories are called on and experienced, and where love, hate, jealousy, ambition, mastery, competitiveness, and other basic human emotional states are invoked. Biosensing, found at the intersection between physical indicators and brainwave measures, will become the biggest growth area on the internet. In this world, cybersecurity and emotional security will become inextricably intertwined. Cybercriminals, corporations, and governments will not only take advantage of tracking human emotion but also begin to subtly manipulate those emotions for licit and illicit gain.

THE WORLD

This scenario portrays a world of 2020 in which emotional sensing becomes a central—and possibly the central—feature of internet technologies. The precursors to this world are already in place in 2016. Consider the "Quantified Self" movement, a hobbyist trend toward using technology to measure unexpected aspects of daily life.[1] In this world, the movement will lose its name by 2018 because its practices will become mainstream. Just as smart phones became standard possessions over the course of a few years, biosensing devices will become ubiquitous as the price of sensors that are deployed on and around human bodies falls further.

"Personal metrics"[2] already allow for tracking empirical behavioral patterns. In this world, these metrics will be monetized for commercial products, help achieve personal goals (like fitness), and enable productivity "hacks"[3] for daily life. As these devices become more accurate and the effects more widespread, it will become common in major cities to see people wearing three, four, or perhaps 10 personal metric devices. Implantable devices will be the new horizon for hobbyists, and these too will become mainstream in a short timeframe (though perhaps not by 2020).

Much of this technology—in its first iterations—will make relatively little difference. Step counts and real-time heart-rate data turn out to be mostly curiosities, instructive for improving health (at least in theory), but with limited value to others. Reminders and records of time spent sitting, standing, or talking prove to be clever conversation starters but not much more. For all the money, effort, and attention that will be spent trying to build truly useful products and services on top of these devices and their data streams, success will continue to be elusive. Most wearable devices will end up in someone's drawer after a couple of weeks—for now.

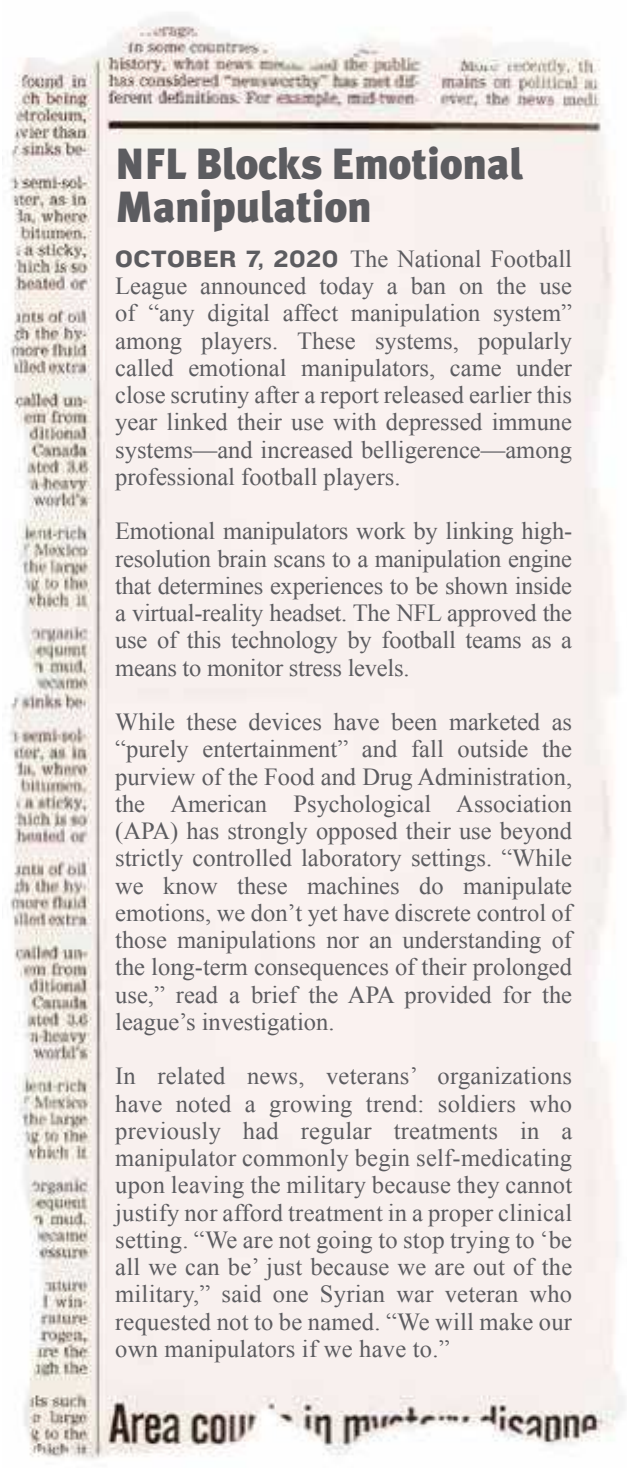
The real turning point will occur when the market for sensors shifts to include not just personal wearables and data trackers, but an extensive array of remote sensors that capture data about interactions between significant numbers of people. So-called sentiment analysis already allows firms to detect shifts in public opinion based on reactions to events online.[4] When that data can be combined with, for example, heart-rate variability data and extensive external information about what is happening to the people whose heart rate is being tracked at that moment, the value of measuring interactions will explode. When body temperature, brainwave activity,[5] eye-tracking and pupil dilation, perspiration, endocrine and glucose levels, endorphin highs, and other variables can be measured through portable devices and among groups of people who are interacting in a particular environment, it will become plausible to understand interpersonal dynamics better than ever before. As sensors get better and smaller, these recording devices likely will not be visible to the naked eye; imagine brain sensors on the earpiece of the latest Kate Spade glasses, or contact lenses that can measure not only glucose but also other biomarkers in eye fluid.

The real turning point will occur when the market for sensors shifts to include . . . remote sensors that capture data about interactions between significant numbers of people.

This will mark the rapid launch of a new research field, combining aspects of clinical psychology and computer science and focused on individual "affects," or surface impressions of an individual's mental state. Think of today's efforts to use facial cues to measure emotion but scaled up, occurring in real time, and made extremely precise. The promise of this field will generate a second round of interest and investment in personal metrics. Doctors will use these capabilities for the long-term health monitoring of patients on a much broader platform; companies will use them to study productivity and performance patterns of employees and teams; marketers will use them to reach a new level of customized advertising and product placement; school systems will use them to help identify deeper sources of learning patterns and behaviors in students; and communities will use them to understand what is actually happening and what citizens really care about.

What will enable these kinds of developments? Progress on these dimensions will be a function of knowing not just what people do and say but also how they feel at each moment. Data about emotional states will be the key that unlocks the latent value of personal and professional data already being collected in 2016. In other words, analysis at the intersection of internal (personal) and external (environmental) outcomes will reveal extraordinary details about how people respond to one another and to stimuli in their environment. Researchers will be able to measure and record the landscape of human emotion—its conditions, triggers, and effects. Interest in aggregated insights—the "emotional internet"—will begin to supplant interest in individual affect as analysis becomes more sophisticated. Surface impressions of people's emotions will no longer be interesting, because the underlying emotions themselves can be measured precisely, at scale, and with very high accuracy.

FROM THE FUTURE



NFL Blocks Emotional Manipulation

OCTOBER 7, 2020 The National Football League announced today a ban on the use of "any digital affect manipulation system" among players. These systems, popularly called emotional manipulators, came under close scrutiny after a report released earlier this year linked their use with depressed immune systems—and increased belligerence—among professional football players.

Emotional manipulators work by linking high-resolution brain scans to a manipulation engine that determines experiences to be shown inside a virtual-reality headset. The NFL approved the use of this technology by football teams as a means to monitor stress levels.

While these devices have been marketed as "purely entertainment" and fall outside the purview of the Food and Drug Administration, the American Psychological Association (APA) has strongly opposed their use beyond strictly controlled laboratory settings. "While we know these machines do manipulate emotions, we don't yet have discrete control of those manipulations nor an understanding of the long-term consequences of their prolonged use," read a brief the APA provided for the league's investigation.

In related news, veterans' organizations have noted a growing trend: soldiers who previously had regular treatments in a manipulator commonly begin self-medicating upon leaving the military because they cannot justify nor afford treatment in a proper clinical setting. "We are not going to stop trying to 'be all we can be' just because we are out of the military," said one Syrian war veteran who requested not to be named. "We will make our own manipulators if we have to."

Consumers initially will be wary of the incredible intimacy this new stream of activity seems to convey. Their ambivalence will be tested repeatedly and sometimes unintentionally. For instance, Fitbit and Jawbone might together release a "mood armband" that, despite enormous media and scientific attention, surprises with its slow uptake in the market. Consumers will wonder whether this device is, on the one hand, actually able to do what it claims, or perhaps, on the other hand, able to do more than it claims: could it allow the firms behind the device to learn more about our emotions than we ourselves know? That ambivalence will be mixed with skepticism about whether emotional tracking is anything more than a gimmick—or even a farce.

This mix of fear and skepticism will linger until companies decisively prove the value of this new technology. Facebook might release, with great fanfare, a "Mood History" product that periodically reminds users of their mood on any particular day up to two years ago. The program would be accompanied by a premium offering that claims to be able to predict mood on days going forward, and suggests behaviors that individuals can employ to make themselves feel more settled, calm, and even happier over the course of a day. The idea would seem so audacious that no one would take it seriously—until they try it and find out that it works.[6]

FROM THE FUTURE

MOOD HISTORY: THE NEXT STEP IN QUANTIFIED SELF?

"Mood History" would enable a Facebook user to record and reflect on his moods over time.

Such proof will signal a tipping point in the marketplace. A new horizon of devices and applications will be developed, focusing on what can be done with reliable measures of emotional insight at scale. Some of the use-cases will be almost mundane: it will be much easier to know if your date is having a good time, or if party guests are enjoying themselves as much as they want you to think they are. Some will be fascinating: how do your employees really feel about working for you? How deep is the loyalty of Chicago Cubs fans to a team that hasn't won a World Series for decades? Some will be deeply personal: does my spouse really like the gift I gave her? And some will prove incredibly useful in day-to-day interactions where emotional states are hard, but extremely valuable, to communicate. Imagine replacing the 10-point scale for pain with the ability to convey to a physician precisely how much an injury or disease hurts, frightens, or troubles you.

A new horizon of devices and applications will be developed, focusing on what can be done with reliable measures of emotional insight at scale.

From the seemingly trivial to the most serious, information about fundamental aspects of emotional experience will become newly accessible. For many, it may feel less like a revolutionary development than the next incremental technological advancement. The irony is that the technology will be able to gauge exactly that dimension of response to itself. Might this be the new frontier in machine-learning—a system that can self-adjust to stay on the "comfortable" side of the human response equation to maximize adoption of itself?

OUTCOMES

The ability to use physiological and sensor data to accurately gauge human emotion will still seem a novel and preliminary capability in 2020, and the extent to which this data can be used to make deeper, long-term causal inferences about behavior will be a source of debate among experts. But for many practical applications, the technology will outpace expectations and yield a stream of surprises. The first stage of adoption will see a wide variety of new uses for broad but fairly shallow emotional sensing across myriad sectors. Governments will respond by seeking to regulate the extreme cases without slowing innovation (a familiar trope). Cybersecurity tensions will run high in this world, as illicit actors and their opponents experiment boldly with what they can do to predictably and controllably influence human emotion.

Uses of Emotional Sensing

The promise of new emotional sensing technologies will inspire a wide variety of initiatives to improve both lives and profits. The icon of this world might be the app for "emotionally verified emojis," released by Apple in 2020 as the primary feature of its newest mobile operating system. But this world would be about much more than just emojis that tell the truth.

In the healthcare industry, psychologists could seek to access a historical record of emotional incidents to create a "digital emotional memory." Such a record could allow health professionals to more accurately explain the circumstances that lead individuals toward mental states like depression, and, by tailoring care to those needs, could vastly improve the mental health of the population. Imagine the improved life experience (and economic productivity gains) of an American population with rates of depression reduced by even 10 percent.[7] On the less positive side, for some people the constant recording and reporting of emotion will create a

FROM THE FUTURE

Dr. SmartWatch

+ New sensor system lets you send emotionally verified emojis!
+ Integrates periodic snapshots of your face to feed into Facebook's Mood Tracker®.
+ Contains FDA-approved glucose and hormone-level tracking.
+ Integrates seamlessly with Mood Governors required in new cars and trucks.
+ Advanced sentiment analysis can analyze the moods of people around you.

Retail Price: $400

self-fulfilling prophecy, as negative feelings and mind-states are reinforced—though it likely will not be possible for some time to separate individuals who benefit from those who are harmed. It may also become possible to foresee forms of addiction within emotionally quantified lives, including new levels of dependency on the aid and stimulation of neurochemical reward pathways. People may grow increasingly dependent on endorphin highs, whether they come from over-exercising, bullying, or shooting weapons.

Realms in which individual performance is held to extraordinary standards will have early and high-intensity exposure to new emotion-sensitive technologies. Professional athletes will seek out new monitoring programs to achieve peak confidence and emotional energy at game time. The military will press the boundaries of similar programs for use in combat. CEOs and political figures will give up their life coaches in favor of emotion-sensing advisement. There will be significant incentives to impose new regulatory regimes in these areas, as those with access to the best technology (or the guts to try it out) may develop meaningful advantages in many domains. Would NFL owners in 2020 argue about whether to ban some of these technologies as "performance enhancing" in the same way the NFL banned steroids and human growth hormone years earlier?

At less intense levels of deployment and usage, the emotional internet will bring on new needs for individuals to manage their emotional public image, which will become part of basic social maintenance, given employer and social interest. Individuals will "groom" themselves to produce positive physiological signals that display how calm, happy, and adventurous they are throughout the day. A new profession—the mood coach—might arise to offer services aimed at helping individuals keep their measurements within a desirable range.

The destabilizing effect these emotional tools may have on interpersonal relationships will be a source of much fascination, though it will be difficult for researchers to determine how much of the effect comes from emotional manipulation alone, compared to the broader shift toward digital communication as a whole (e.g., using social media for relationships or texting as a primary form of communication). Thus, despite all of the suspicions and media attention on what could go wrong, those who want to "turn back the clock" on the emotional internet will struggle to create a unified narrative (at least in the West). Overall, people will feel that the social benefit and utility provided by this data outweighs the potential risks, and the apparent economic advantages will continue to drive ambitious research and development.

At less intense levels of deployment and usage, the emotional internet will bring on new needs for individuals to manage their emotional public image.

By 2020, a person's "memories" of events or periods in their life will be to a surprising extent verifiable by their own data record—not just the facts, but also the tonal quality of the emotional experience that took place. Many aspects of these records will be available not only to the users themselves but also to other sensor systems operated by companies, governments, and other individuals with whom a person had close contact. The records will be attractive targets to attack—to steal, manipulate, or hold hostage.

FROM THE FUTURE

Worried about your public emotional profile?

Consider hiring a Mood Coach!

Managing your emotional public image and outward mindset appearance is crucial for anyone looking to get ahead.

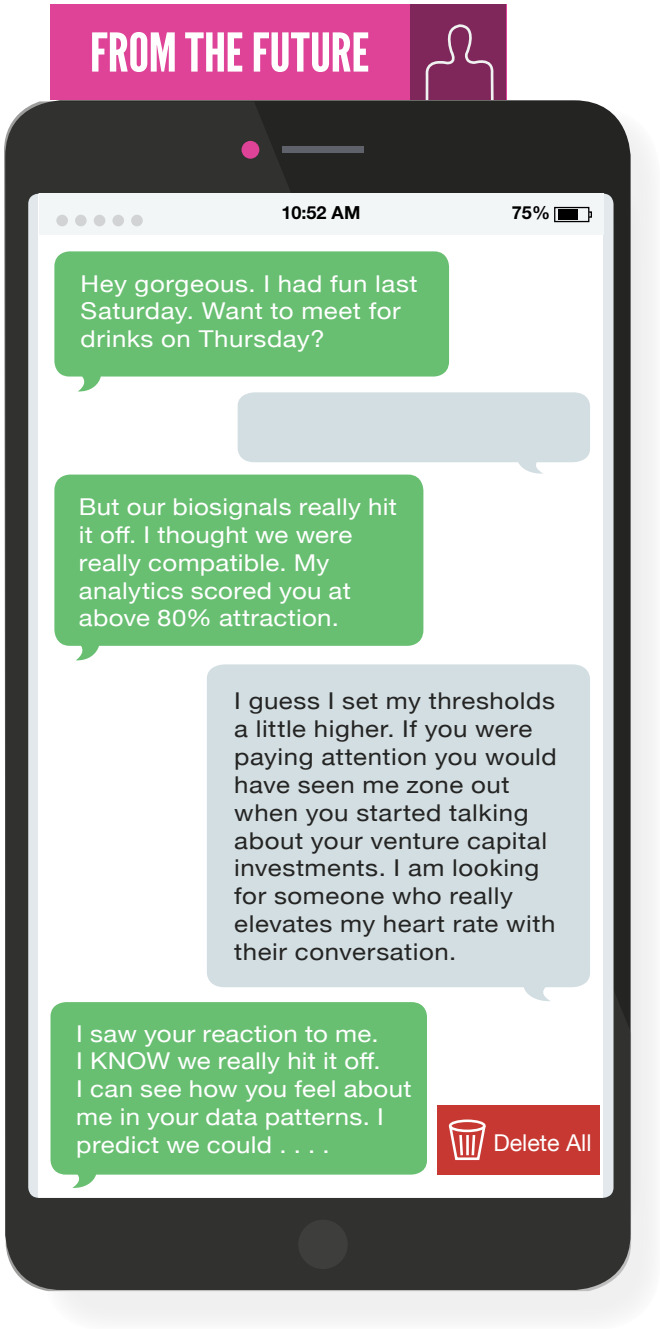
Our certified Mood Coaches can help you send out positive physiological signals, whether you're hoping to convey calm confidence or mask that you're falling in love.

Private-sector organizations will push the field forward at scale. Measurable improvements in decision-making and team performance will be sought and sometimes achieved, though the precise causal links between emotional states and "quality" decisions will remain tricky to establish. Markets will start to value at a premium firms that make these technologies or use them in leading-edge ways. Can corporations limit interactions between employees based on analysis suggesting their personality types are incompatible? Can someone be fired as an at-will employee based on emotional analyses? The public sector would not be far behind. Imagine in 2020 a leading US politician announcing that when she has to make hard decisions, she calls her behavioral psychologist for advice, rather than her best friend or priest.

The boundaries between licit and illicit transactions will become blurry in this world. Does a firm that wants to hire analysts of a certain Myers-Briggs Type Indicator[8] for a particular team cross the line when it buys access to a proprietary algorithm that pulls out candidates with that indicator from a consolidated database, rather than taking the (much less accurate and scalable) approach of simply administering the Myers-Briggs test to potential hires? Competition among dating services will push toward what some will see as unsavory and illicit practices—for example, when preferences around emotional control and manipulation in relationships become reliable and priceable product features. It might be nice to know "for certain" that your dream date will be interested in emotional attachment that evening. But what if that product turns out to give the wrong signal even one time out of 50?

In a world where emotional sensing is commonplace, so too are the opportunities for intentional manipulation, both of the sensing systems and of raw emotions themselves. Vulnerabilities will come in many shapes and forms: emotional manipulations that human beings have always tried to impose on one another will become more systematic, targeted, and effective, and so will emotional countermeasures. As this arms race ratchets upward, we may start to see evidence of an "overclocking" of affective systems that occurs as emotions become separated from and imbalanced within the larger human cognitive and physical systems. Put differently, these kinds of emotional capabilities could easily outpace the evolutionary ability of humans to manage them in concert with other mental and physical systems. If all decision-making is a combination of cognitive and emotional processing,[9] what happens when one of those two components suddenly starts moving much faster than the other?

Such a rapid (in evolutionary terms) reconfiguration of what a critical part of the human mind can do will present a vast attack surface for deception and manipulation, creating an entirely new "field" of emotional crime. It is one thing to commit identify fraud and steal money or property from a person; it is another thing to subtly manipulate an emotional state so that the victim "voluntarily" hands over money or property to a criminal because she feels she really wants to "contribute" to a "cause"—or to confuse or disorient the victim in deep emotional ways, leading to the same result. The ability to carry out these kinds of manipulations against multiple individuals simultaneously with targeted interventions cannot be explained away as a better form of advertising or propaganda; this will be something of a different kind.



The integrity of emotional data will also be in play in a different way—through rewriting history. In 2019, reports might emerge of high-profile individuals faking their own data profiles and retrospectively altering their emotional histories through database hacks at large sensor companies. Could a future presidential candidate be accused by his competitors of falsifying his emotional history to cover up prejudice and malice toward particular groups of individuals? Coupled with some random (or perhaps systematic—who can know for certain?) sensor error, it will become increasingly difficult for individuals to prove that their emotional records are truthful—not only to others, but also to themselves in some instances. Garmin might be taken down in a weeklong distributed denial of service (DDOS) attack by the "Anti-Hysterics," a group known for their public protest of large-scale emotional analysis. The public response might be muted as people try to figure out who the good guys really are. Will a new market for sensor-blocking technologies emerge to enable individuals to "opt out" of sensor arrays designed to compute their emotional states?

Legal and Policy Regimes

It is difficult to imagine that contemporary beliefs and practices around privacy would survive the transition toward the emotional internet. More likely, privacy arguments from earlier in the decade will come to be seen as quaint, because what will be at stake in 2020 are some of the most fundamental questions about what is public and what is private, what is intimate and what is not. The boundaries between legitimate and illegitimate action will now have to be negotiated at an entirely new level.

Some observers will argue that emotion is already exposed in the public realm during normal human interactions and thus cannot be privileged under any kind of "reasonable expectation of privacy" standard. Remote sensing or sensing at some distance (Is an airplane passenger overly nervous? Is a now-peaceful protestor's anger approaching some threshold?) might not have any effect on that argument as long as the sensing takes place in settings that are generally thought of as public. The private sector will try to keep the game wide open by deploying familiar "innovation permission" arguments (that is, arguments favoring greater flexibility for those who are innovating), pointing to the range of goods and services that are improving people's lives and encouraging regulators to stand back. If they succeed, privacy advocates might end up fighting on the margins, emphasizing the need for protections against emotional tracking in private spaces, as well as protections for particularly vulnerable populations—like children, the mentally ill, and older people suffering from dementia—whose emotional data records might need to be "clean-slated" at some appropriate moment.

Some observers will argue that emotion is already exposed in the public realm during normal human interactions and thus cannot be privileged under any kind of "reasonable expectation of privacy" standard.

At the same time, businesses (legal and otherwise) that capitalize on some of the more base or unseemly aspects of human behaviors—from pornography to fear and terror inducement—will be at the forefront of experimentation and, as is usually

the case, will find ways to route around whatever boundaries are established by law and regulation. If establishing a contract requires a "meeting of the minds" between freely deciding individual parties to a negotiation, where does emotional data about the history of the parties, or their interactions in a particular case, move from efficiency-enhancing to something more insidious? Would a murder trial in 2020 allow biosensing evidence as part of a heat-of-passion defense?

The lack of any overarching theory about emotional data makes it more likely that regulation in the United States will evolve in the same stove-piped and segmented way that "normal" information privacy laws have developed. Health uses of biosensing data will be protected to some extent under amendments to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and health privacy policies; these might also extend to protect individuals from particular kinds of discrimination based on emotional health. Even so, there will be huge fights over the boundaries of both "emotion" and "health." Student privacy laws might restrict the use of emotional analytics to very particular educational purposes, and also limit access and retention of these records (unless it turns out that data about emotions makes a huge difference in performance).

Employees are less likely to be protected from emotional performance evaluations or job hiring screenings, in which case the use of biosensing devices in the workplace could become the norm. Labor unions might find new life as a bulwark against some of the more egregious uses of sensing data in both blue- and white-collar workplaces. The proliferation of emotion sensors in public spaces also would generate a significant increase in liability and harassment suits, since combined physiological and emotional data could be used to back up legal claims. This will create a seemingly inconsistent and confusing landscape of regulation that is much harder to navigate than anticipated.[10]

Labor unions might find new life as a bulwark against some of the more egregious uses of sensing data in both blue- and white-collar workplaces.

At a more local level of governance, intrusive regulatory interventions will likely emerge first to deal with situations where emotional states are associated with high-stakes and irreversible decisions that can be marked off as discrete events. Imagine a scandal where an unusual series of individuals get elected to the San Francisco Board of Supervisors after campaign materials are used to manipulate local citizens, who report feeling euphoric and optimistic regarding candidates who are heavily funded by local wearable emotion data startup companies.[11] California might then mandate a cooling-off period (time and space) around election centers to allow citizens to stabilize their mood without stimuli before voting. Other states might regulate the use of emotion-manipulating campaign tactics in the media, or adaptive campaign placards that feed off data from potential voters entering their vicinity. It would not just be about voting: some states might require auto manufacturers to incorporate emotion data into speed limiters on car engines, or even ignition switch-disabling technologies that set an "anger threshold" above which you cannot start your car.

FROM THE FUTURE

Brianna Jones's Diary

4 Mon 5 Tue 6 Wed

8:30 AM EST - Mass-transit commuter train heading into Washington, DC
Heart rate: Normal. Blood pressure: Normal. Caloric counter: On track. Steps taken: 950 to go! Oxygen level: Normal. Alertness: Medium.

I remember in middle school discovering I was a "blusher." Jason Markowitz came up to my lunch table and asked me to the spring fling. I turned as red as my tomato soup.

We are all blushers today. A quickening heart, dilated pupils, minute spikes in body temperature, fluctuating oxygen levels—they all give us away.

I actually like it this way, though. How else would I have known my (now) ex-husband was having an affair without the accumulating signals from his MoodSensor5000, neatly summarized in a monthly report? Sure, he lamented smoothly about his longer working hours - but the sweat glands one layer below his skin gave away his lies.

10 AM EST - Synergy Incorporated
Heart rate: Quickened and variable. Blood pressure: Elevated. Caloric counter: Ready for lunch. Steps taken: Need 600 more. Oxygen level: Normal. Alertness: High.

I didn't get the promotion. Our division director Bob, beaming out biosignals that read as cool as cucumbers, took his time before announcing the new task lead. It's Melissa.

It took every breathing exercise and transcendental meditation I knew to keep my signals at a level where nobody would notice I was freaking out.

Most of us were nudged by our MoodSensor5000 to reach out to Mark Jones and offer a joke or reassuring affirmation. Mark really should have taken that mood stabilizing workshop last month. I really got my money's worth out of that.

Today

4 PM EST - At my desk
*Heart rate: Above average. Blood pressure: Elevated. Caloric counter: Close to daily maximum. Steps taken: Need 300 more. Oxygen level: Normal. Alertness: Medium.*Phone rings. "Hi this is Phyllis, the school nurse. Sutton needs to be picked up from school. There was a problem with his sensors."

"What do you mean? I've been watching them all day from my work computer. He seems fine."

"Well, we intercepted a group of boys using an emotional stingray. They were falsifying his data, so neither the school nor his teacher knew he was becoming overstimulated."

<Interruption> "I want them expelled!"

"Ma'am, they are in detention being given the maximum amount of discomfort and understimulation we are allowed to administer by law."

Click.

4:30 PM - Leaving work early to pick up Sutton
Heart rate: High. Blood pressure: High. Caloric counter: Close to daily maximum. Steps taken: Need 250 more. Oxygen level: Normal. Alertness: High.

Still fuming over not getting the promotion. I knocked on Bob's glass door. I hated how perfect his levels still read.

"What can I do for you?" he inquired, evenly.

"My performance numbers are far above Melissa's. We have comparable skill sets and experience levels and . . ." I trailed off.

He grinned. "We've been remotely monitoring the biosignals employees expend in front of clients. Your file is full of high stress and negative energy. You really brought down the 'energy stats' posted on our website. You need to work harder at regulating your mood and physiological readings, because . . . "

Before he could finish, my MoodSensor5000 began squealing. My blood pressure spiked so high it kicked into emergency notification mode.

FROM THE FUTURE

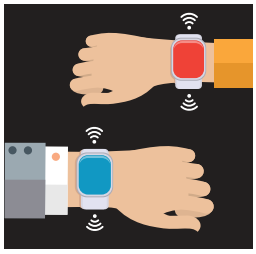
http://www.denverchronicle.com/privacy-advocates.html

The DENVER Chronicle

News | Hot Topics | Columnists | Companies | Special Reports | Marketplace | Tools | Contact | Blog

OCTOBER 15, 2018

Privacy Advocates Concerned About Government-Sponsored Wellness Trackers



A newly proposed federal program that would provide free wellness-tracking devices to Medicare and Medicaid recipients has come under fire after it was revealed the program would enable the government to monitor not only the day-to-day location, activity, and physical health of millions of Americans, but also some rough indicators of their happiness levels.

The "Get Fit, Bit by Bit" program, an initiative developed by the Department of Health and Human Services (HHS), would provide up to a 15 percent discount on medical services to patients who agree to wear the devices, as well as a $50 cash incentive for wearing them for six months.

Sarah Johnston, HHS's under-secretary for digital wellness, defended the program. "For years, companies have provided their employees with these kinds of devices to nudge them toward improved health, and both the companies and the employees enjoyed reduced insurance rates as a result," she said. "We are just extending this to Medicare and Medicaid patients."

Privacy advocates argue that the government should not have access to the kinds of personal information commonly captured by the armbands—and that the low-income Americans most likely to use public health insurance will be disproportionately vulnerable to being monitored. "If a government official wants to know if I'm happy about a new law they want to pass, how about they do something crazy and just ask me?" said John Swenson, a Colorado privacy advocate.

The criticism is part of a wider backlash against the devices. Last week, officials from the Service Employees International Union (SEIU) voted to disallow the devices in workplaces where their members are employed out of concern that companies were monitoring people's mood states surreptitiously.

Meanwhile, international watchdog organizations are challenging a recent program by the World Health Organization that would deploy millions of solar-powered health and emotion sensors in the developing world, arguing that Western nations will inevitably try to use the data for intelligence purposes.

Beyond US borders, the landscape of experimentation and regulation would become far more complex. Transatlantic arguments about issues that are prominent in 2016, like "Safe Harbor" data protections and the competitive dynamics of large, US-based intermediation platforms such as Uber and Airbnb, would seem pedestrian compared to the differences that would likely emerge around emotional analytics. Might Germany simply try to ban the use of remote emotional sensing and create protected categories (e.g., students or employees) where even local or personal sensing data could not be utilized? Would the European Union demand an even more stringent set of protections?

Conversely, will some of the faster-growing emerging economies in Africa and Asia move to accelerate the deployment of an "emotionally intelligent infrastructure" as they seek to leapfrog the competition with productivity and new products and services? Autocratic regimes will certainly want access to their population's emotion datasets for many reasons, including control and manipulation. In his advice to the Prince, Machiavelli famously said that it is better for a ruler to be feared than to be loved, so long as fear does not corrode into hatred.[12] Imagine a world where ambitious autocratic rulers could calibrate these variables to precise measures of how populations respond to what they do.

Cyber-Emotional Security

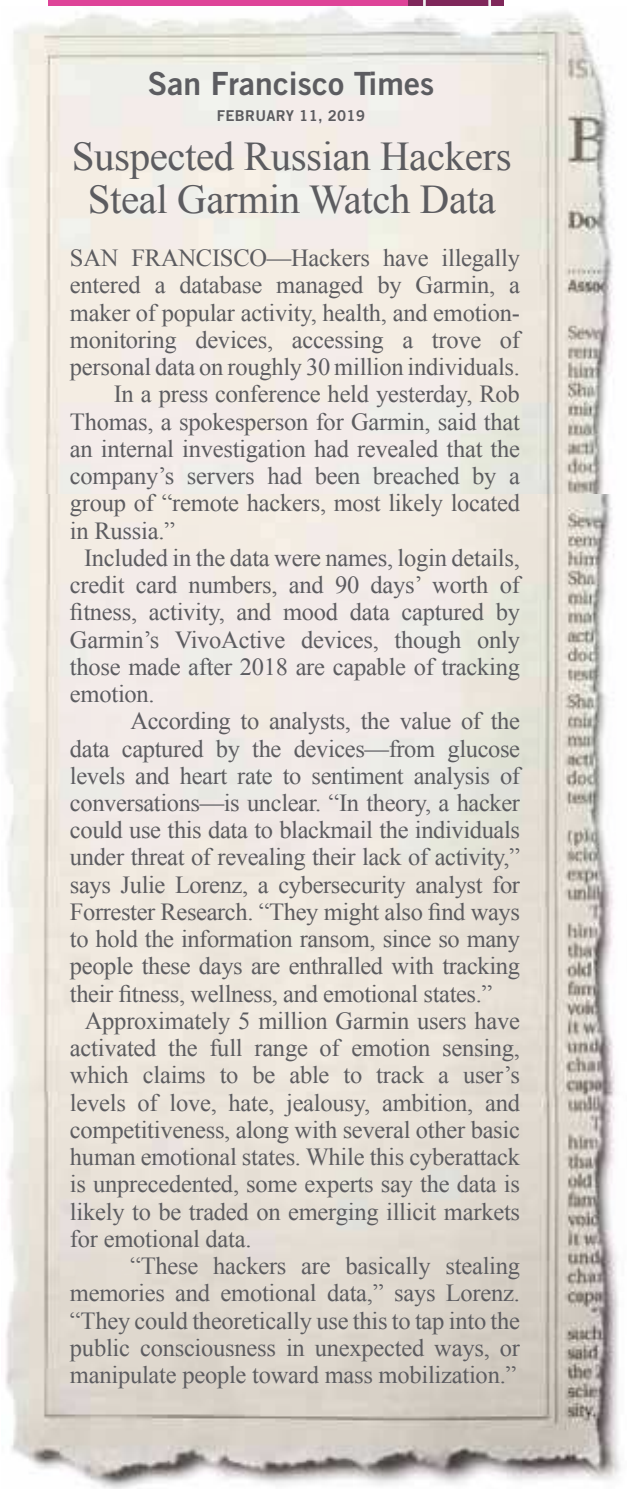
In this world, the possibilities for communicating more effectively, working together, managing conflict, and assessing customer experience are hugely compelling. But so are the possibilities for manipulating emotional states, stealing and reconfiguring memories, using emotional datasets for mass mobilization toward the manipulator's ends, and other assaults on this new and massive attack surface. This is a world in which cybersecurity becomes cyber-emotional security.

There are three key aspects to cyber-emotional security: device insecurity, emotional manipulation, and the vulnerability of data. On the first point, one core attack vector will be to target devices themselves, many of which will be made by companies with limited security experience. Implantables will be particularly vulnerable, given the difficulty of removing them to fix hardware. Other sensitive targets will involve devices related to advances in medicine expected to take hold toward the end of the decade. Will hackers be able to attack digital storage devices containing individual DNA datasets, or 3D printers (and their build files) that construct the substrates for new organs?

Second, many traditional cyberattack vectors will expand in this world to involve much more effective and precise manipulation of emotions. Phishing? Attack someone with a word or phrase that is not just familiar, but particularly emotionally compelling. Social engineering thus becomes emotional engineering. Cybercriminals will also see significant benefits from attacking the new emotional sensing systems directly. Want to decrease productivity at a particular company? Manipulate team selection engines so people with incompatible traits have to work together, or worse, manage one another.

Finally, as this world develops, the value of the data being stolen will increase. While easily accessible, data from personal network devices and "quantified selves" will not be very interesting to criminals. How your mood changes at different times of the day may be harder to steal and interpret, but if done well, will be much more interesting and lucrative. It is possible to foresee a segmented market for illicit data at different points in the value chain: raw quantified self data, like raw coca leaf, will be cheap, while emotional information that can be used will be expensive, like cocaine.

FROM THE FUTURE



San Francisco Times

FEBRUARY 11, 2019

Suspected Russian Hackers Steal Garmin Watch Data

SAN FRANCISCO—Hackers have illegally entered a database managed by Garmin, a maker of popular activity, health, and emotion-monitoring devices, accessing a trove of personal data on roughly 30 million individuals.

In a press conference held yesterday, Rob Thomas, a spokesperson for Garmin, said that an internal investigation had revealed that the company's servers had been breached by a group of "remote hackers, most likely located in Russia."

Included in the data were names, login details, credit card numbers, and 90 days' worth of fitness, activity, and mood data captured by Garmin's VivoActive devices, though only those made after 2018 are capable of tracking emotion.

According to analysts, the value of the data captured by the devices—from glucose levels and heart rate to sentiment analysis of conversations—is unclear. "In theory, a hacker could use this data to blackmail the individuals under threat of revealing their lack of activity," says Julie Lorenz, a cybersecurity analyst for Forrester Research. "They might also find ways to hold the information ransom, since so many people these days are enthralled with tracking their fitness, wellness, and emotional states."

Approximately 5 million Garmin users have activated the full range of emotion sensing, which claims to be able to track a user's levels of love, hate, jealousy, ambition, and competitiveness, along with several other basic human emotional states. While this cyberattack is unprecedented, some experts say the data is likely to be traded on emerging illicit markets for emotional data.

"These hackers are basically stealing memories and emotional data," says Lorenz. "They could theoretically use this to tap into the public consciousness in unexpected ways, or manipulate people toward mass mobilization."

Since firms will probably be the first to exploit these new data assets legally at scale, workers inside retail, advertising, entertainment, and pharmaceutical companies who try to use this emotional data for nefarious purposes will be a huge threat. Companies collecting the most robust datasets will also be vulnerable to attack.

In contrast, many governments will likely fall behind in the exploitation race; for democracies and others that care about public reactions, the "creepiness" factor of this data will be very high. Authoritarian governments will want to much more aggressively monitor the mass emotional states of citizens and test responses to stimuli—and their adversaries will want to steal that data. Surely intelligence agencies in Western countries would deeply value access to the Chinese government's longitudinal data on Chinese citizens' happiness and frustration.

. . . workers inside retail, advertising, entertainment, and pharma companies who try to use this emotional data for nefarious purposes will be a huge threat.

Terrorists will be very interested in emotional data, both as an attack vector and as a way to identify the intensity of beliefs among their adherents (as well as to identify possible moles among potential recruits). It may be that the barriers to reliable interpretation are high enough that only the most sophisticated groups would go down this road, but some will surely try.

Familiar tradeoffs around security will appear again in this new domain, potentially with much higher stakes. Facebook (or its successor) will jump on the fact that individuals will want to "send" feelings and experiences to their friends and colleagues, as well as receive the same in return. The system that measures, captures, transmits, and interprets these emotions will want to ensure the availability and integrity of that data at all levels, from the individual upward. But individuals may also look for new means of emotional confidentiality, or sentiment protection, for mind states they do not want exposed in public. This tension would likely present first as a desire for some preservation of emotional privacy, but it will be extremely hard to define these parameters in advance.

Possibly the greatest risks will start to manifest in services that offer manipulation of emotional states and memories, even if by intention for the good of the user. The question of how users of these services can know that they will receive (or have received) the "manipulation" they want and not some (possibly subtle) variation that serves someone else's ends may be the most critical new cybersecurity question. The broader uncertainty may start to be seen as a question of whether emotions remain useful and reliable tools for understanding the people and the world around us. This will be especially true as nation-states start to see the potential to use emotional states as large-scale, targetable, and reliable weapons.

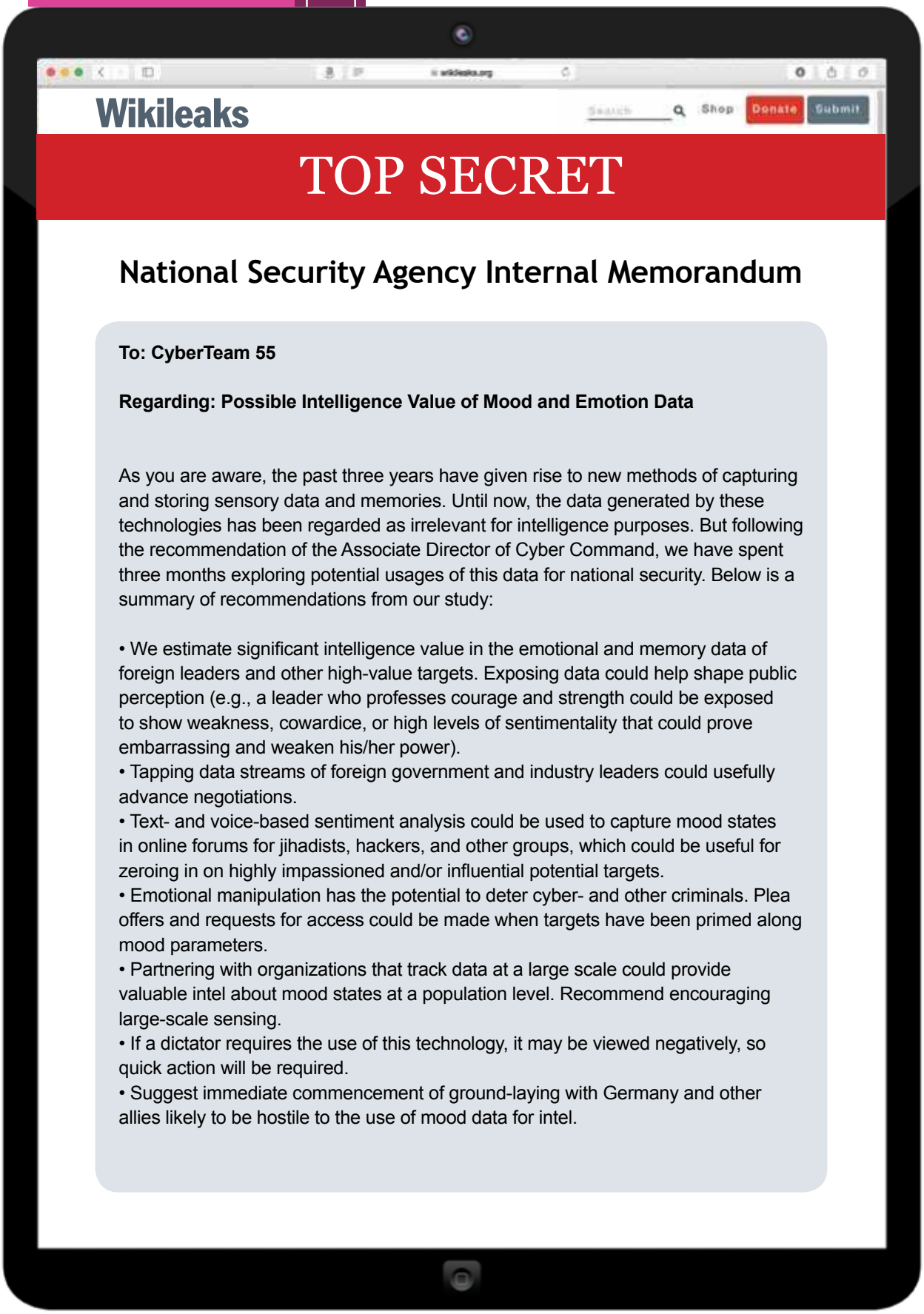
It is likely then that traditional and newly formed response groups will focus on developing distinct strategies for preserving security in relation to malevolent actors, firms, government agencies, and society at large. Individuals will want not only to protect certain data from being recorded but also to confirm the truth of the data that they do release. ("Yes, honey, I really do like that dress.") New corporations promising third-party validation of emotional data will seek to provide such confirmation. Protecting the largest troves of emotional data also will be a priority of governments; such information may even be categorized as critical infrastructure, and thus in some cases might fall under the protection of the state.

. . . risks will start to manifest in services that offer manipulation of emotional states and memories . . .

The relationship between hackers and their targets will also shift. Hackers would almost certainly go after the emotional data of high-profile individuals to try to expose their mind states to show hypocrisy. Defense departments and private-sector cybersecurity companies, meanwhile, will expand the concept of deterrence to include the emotional states of the cybercriminals and warriors at the other end of the network, because emotional manipulation will become a key driver in preventing cyberattacks.

As ever, response efforts will mix technology with regulation, and will seek to shift social norms around what is "appropriate" behavior and action in particular environments. Governments will now have a huge new tool in the war for public opinion. Will counterinsurgency funding in places like Iran and North Korea shift into the mass emotion-manipulation domain? Or could the emotional status of particular foreign leaders be targeted on an ongoing basis? The results will be mixed, not least because this is a fundamentally new playing field. Communication about emotion has always been remarkably difficult, and it will take quite some time for people to understand what some of these new capabilities and insights truly mean.

FROM THE FUTURE



National Security Agency Internal Memorandum

To: CyberTeam 55

Regarding: Possible Intelligence Value of Mood and Emotion Data

As you are aware, the past three years have given rise to new methods of capturing and storing sensory data and memories. Until now, the data generated by these technologies has been regarded as irrelevant for intelligence purposes. But following the recommendation of the Associate Director of Cyber Command, we have spent three months exploring potential usages of this data for national security. Below is a summary of recommendations from our study:

• We estimate significant intelligence value in the emotional and memory data of foreign leaders and other high-value targets. Exposing data could help shape public perception (e.g., a leader who professes courage and strength could be exposed to show weakness, cowardice, or high levels of sentimentality that could prove embarrassing and weaken his/her power).
• Tapping data streams of foreign government and industry leaders could usefully advance negotiations.
• Text- and voice-based sentiment analysis could be used to capture mood states in online forums for jihadists, hackers, and other groups, which could be useful for zeroing in on highly impassioned and/or influential potential targets.
• Emotional manipulation has the potential to deter cyber- and other criminals. Plea offers and requests for access could be made when targets have been primed along mood parameters.
• Partnering with organizations that track data at a large scale could provide valuable intel about mood states at a population level. Recommend encouraging large-scale sensing.
• If a dictator requires the use of this technology, it may be viewed negatively, so quick action will be required.
• Suggest immediate commencement of ground-laying with Germany and other allies likely to be hostile to the use of mood data for intel.

THE WAY FORWARD

This is a world in which sensors become capable of identifying and tracking emotional shifts in individuals at a large scale. In such a world, corporations that engage in and offer emotional tracking as a service will see economics benefits; politicians will explore new campaign tools; and criminals will identify vulnerabilities presented specifically by the no-longer-so-mysterious landscape of human emotions. Cybercriminals will not only take advantage of tracking human emotions but, in subtly learning to manipulate them, will create an almost entirely new playing field for defenders to manage—without a great deal of clarity, in many cases, around exactly what it is they are defending against.

In this scenario, members of the cybersecurity research community will wish that, in 2016, they had been working on:

MODELING

Identifying the underlying components of emotions and how they can be modeled in the datasets produced through a broad range of sensors

RISKS AND BENEFITS

Understanding the risks and benefits that the proliferation of relevant sensors may represent, including potential criminal manipulation of the sensors and data they generate and the attack surfaces on which they can be

DEFINING SECURITY

Defining the security characteristics of data beyond today's domain-specific concerns, because medical, financial, and national-security data will no longer be defined by these category-specific divisions, but by the effects that such data can have on emotional states

BALANCE

How to balance openness to innovation with various necessary regulatory protections in a realm as poorly understood as the digitization and storage of human emotion

SCENARIO 5 FOOTNOTES

1. See "The Quantified Self," *LiveScience*, accessed March 25, 2016, http://www.livescience.com/topics/quantified-self.

2. See Jason Bellini, "Wearables: Our Personal Metrics Headed to the Cloud," *Wall Street Journal* video, 2:24, October 29, 2014, accessed March 25, 2016, http://www.wsj.com/video/wearables-our-personal-metrics-headed-to-the-cloud/44410AB9-13F1-4A13-AFEB-67287D28F5C2.html.

3. At least one social entrepreneur is working on a book describing "productivity tips/hacks using your iPhone." See Ramit Sethi, "Looking for Productivity Tips/Hacks Using Your IPhone—Suggestions?" *I Will Teach You To Be Rich*, June 22, 2008, accessed March 25, 2016, http://www.iwillteachyoutoberich.com/blog/looking-for-productivity-tipshacks-using-your-iphone-suggestions.

4. See Alex Wright, "Mining the Web for Feelings, Not Facts," *The New York Times*, August 23, 2009, accessed March 25, 2016, http://www.nytimes.com/2009/08/24/technology/internet/24emotion.html?_r=0.

5. Techniques such as electroencephalogram (EEG) and functional near-infrared spectroscopy (fNIRS) already make such measurements possible on a small scale. The difference here will be the availability of such tracking ability in portable devices and on a large scale.

6. "Google Secures Patent for Glucose-Sensing Contact Lens," The diaTribe Foundation, April 16, 2015, accessed March 25, 2016, http://diatribe.org/google-secures-patent-glucose-sensing-contact-lens.

7. Depression is estimated to cost the United States $210 billion per year. See Paul E. Greenberg, "The Growing Economic Burden of Depression in the U.S.," *Scientific American's MIND Guest Blog*, February 25, 2015, accessed March 25, 2016, http://blogs.scientificamerican.com/mind-guest-blog/the-growing-economic-burden-of-depression-in-the-u-s/.

8. For more detail on the Myers-Briggs personality test, see "MBTI Basics," the Myers & Briggs Foundation, accessed March 25, 2016, http://www.myersbriggs.org/my-mbti-personality-type/mbti-basics.

9. See, for example, Antoine Bechara and Antonio R. Damasio, "The Somatic Marker Hypothesis: A Neural Theory of Economic Decision," *Games and Economic Behavior* 52 (2005): 336–372.

10. Campaigns are already using interactive billboards to collect responses from the electorate. See Kevin Randall, "Neuropolitics, Where Campaigns Try to Read Your Mind," *The New York Times*, November 03, 2015, accessed March 25, 2016, http://www.nytimes.com/2015/11/04/world/americas/neuropolitics-where-campaigns-try-to-read-your-mind.html?smprod=nytcore-iphone.

11. Niccolò Machiavelli, *The Prince* (1532).

12. While security and privacy are often seen to be in tension, here security and privacy work together; security ensures privacy is still possible.

For more information on the Center for Long-Term Cybersecurity or these scenarios, please visit **cltc.berkeley.edu.**

CONCLUSION AND IMPLICATIONS

The future of cybersecurity will in one sense be like the present: hard to define and potentially unbounded as digital technologies interact with human beings across virtually all aspects of politics, society, the economy, and beyond. We built this project on the proposition that both the "cyber" and the "security" components of the concept "cybersecurity" will be in rapid motion during the back half of the 2010s. That motion is more likely to accelerate than to decelerate, but its direction varies widely among our scenarios. That is no artifact of our research process; it is the central point of the work.

We hypothesize that, at some point in the not-so-distant future (if it is not already true at present), cybersecurity will be recognized widely as the "master problem" of the internet era. That puts it at the top of any list of problems that societies face, more similar to a nearly existential challenge like climate change than to an operational concern that technology companies have to manage. That recognition also will bring major changes to how human beings and digital machines interact. One purpose of these five scenarios is to point to some of the changes that may result.

In this work, we have left arguments about straight-up military-to-military "cyberwar" to the side. This was by intention, a modeling choice made to bound the problem. It is clear that cyberwar—or at least cyberconflict—will (continue to) happen, because wars will happen and the internet is a contested arena, just like land, sea, air, and space. Moreover, others already have done a great deal of work on cyberwarfare scenarios that can and should be used alongside this document to complement our more market-, technology-, user-, and public-sector-driven scenario set. We acknowledge that a major war between powerful states fought substantially or even principally in cyberspace would be a discontinuity that could redirect in important ways some of the driving forces that we emphasize. But we have chosen to treat this kind of event as more like an exogenous shock or "wild card" than an underlying trend—at least for now.

We have tried to stretch imaginations just enough to see over-the-horizon glimpses of how the problem set will shift and what new opportunities will

arise. The target date for these scenarios, 2020, is very close in time to the present. Our experience with scenario thinking as a modeling tool suggests two important observations about that fact.

The first is that change generally happens faster than people expect. Although we may all suffer a bit from internet hype-fatigue, especially in light of (sometimes outlandish) claims about exponential rates of change, it remains true that the landscape will probably look more different than we expect, sooner than we expect.

The second observation is that it is easier to envision downside risks than upside opportunities. That makes sense in evolutionary, natural-selection-driven environments, where anticipating potentially damaging risk is an advantage for ensuring survival, but it may not be quite so advantageous in engineered environments where human beings have a greater degree of control. The internet is among the most complex environments that humans have created, but it is still (for now) an engineered environment made up of digital machines that are built and programmed by people. Fatalism is just as dysfunctional in that context as complacency.

It is our hope that these scenarios prompt expansive thinking and discussion—that they generate more questions than answers, more bold research ideas and creative policy propositions than fixed emphatic proclamations about what must or must not be done. With that in mind, we offer below some very high-level summary points and provocations that emerged from this work.

The most insight is gained, of course, when particular actors and organizations use scenarios like these to develop more precise and pointed implications relevant to their own interests, positioning, capability, and risk tolerance. So we hope that readers will ask themselves this: confronted with a landscape of future possibilities that feature the issues these scenarios highlight, what will cybersecurity come to mean from my perspective—and what should I, or the organization(s) that I am part of, do next? Equally importantly, what will I need from basic research and policy in order to achieve the best cybersecurity outcomes I can envision?

THE SCENARIOS: A SUMMARY

	NEW NORMAL	OMEGA
Core Logics	Hackers succeed in accessing most digital systems, and everything online is assumed to be insecure	Predictive algorithms are capable of foreseeing individual actions with a high degree of specificity and accuracy
Implications	• The public adopts a baseline attitude of insecurity and reacts in diverse ways • Some industries benefit, but many revert to pre-digital in some processes • Governments protect sensitive assets by taking them off the network	• The public focuses on the benefits of algorithms • Industries encounter major friction as they shift business models to exploit these capabilities • Governments focus offensive and defensive capabilities on predictions of individual human actions
Cybersecurity Redefinitions and Risks	• Cybersecurity becomes cyber-risk; everything is insecure at some level • "Hacker haven" countries protect criminals • Sensitive systems can no longer be secured in the digital realm, so other forms of security are sought	• Humans are truly the weakest link in the cybersecurity chain • Prediction technologies can lead to new attack vectors • Individual targets may become more interesting and lucrative than organizational targets
Cybersecurity Opportunities	• Greater overall transparency as a norm • Potential for strategic stability through high-level deterrence, where states fear hostile reactions to attacks • "Neighborhood watches" can improve security on a small scale	• Predictive abilities vary by sector, providing opportunities to disaggregate problems • Private companies are likely to get much further ahead of regulators but have much greater security investment incentives

	BUBBLE 2.0	INTENTIONAL IOT	SENSORIUM
	A stock market crash of tech companies leads to fire sales of major data assets to generate cash	The Internet of Things is widely adopted, and governments (not private industry) drive that adoption to provide for the public good	Biosensing and related technologies allow companies and governments to measure, capture, and respond to human emotions accurately
	• The public grows disillusioned with the "Silicon Valley" mindset • Companies and criminals race to gain ownership of underpriced data assets • Governments may take over companies and datasets that are "too big to fail" or are national security risks	• Public optimism about new technology translates into positive attitudes toward governments • Companies struggle not to cede benefits to new market players • Governments use the IoT to tackle public-good issues thought to be intractable	• People treat their emotional profile as part of basic social maintenance • Companies aggressively use emotional engineering to improve productivity • Governments will see benefits in intelligence gathering but also new risks
	• Cybersecurity and data security become intimately intertwined • Criminals seek to exploit datasets and the humans that work on them • Markets for data are changing fast and more easily attacked	• Cybersecurity dissolves into the background, becoming simply mainstream "security" • Device makers struggle to manage a massive array of devices • Hackers look for lowest-common-denominator vulnerabilities	• Cybercriminals and hostile governments find new ways to exploit emotion; licit actors test the boundaries of what is acceptable • Key risks include device insecurity, emotional manipulation, and the vulnerability of data collected
	• Data can be secured when its "provenance" can be proved, and so third-party provenance verification is powerful • Governments can help develop mechanisms for making markets for data more efficient and secure	• A degree of expected failure will be engineered into the system to enhance resilience • Governments can use their newly gained credibility to assist in managing the new diversity of threats	• Response groups will seek to validate emotional data • There is massive attention on and value in figuring out how to understand, measure, and protect the emotional states of human beings

We offer, in conclusion, 10 summary insights from the scenario set as a whole. These insights will have different levels of significance for different readers. We present them as a way to provoke further thinking about the meaning of cybersecurity and its implications in an as-yet unseen future.

1. **Human beings are at the center of technology—and they are imperfect.** Digital technologies are powerful, but not powerful enough to overwhelm either human ingenuity or human stupidity. The "basic hygiene" story about educating people to undertake simple security-friendly behaviors (like using better passwords) in day-to-day life is accurate, but massively incomplete. By 2020, we will see meaningful progress in helping people make smarter choices, or at least be more self-aware about and responsible for the choices they make. But there is no technical or behavioral intervention (or combination) that will stop people from creating insecurity through their actions, any more than there is a completeness proof for perfect software code.
2. **Hackers go mainstream.** Hackers will play an increasingly influential role in shaping the criminal world, as digital technology and physical infrastructure become more closely tied together and integrated into human life. In 2020, digital criminals will not be called "hackers" anymore because they will not be considered a special category; they will just be fraudsters, extortionists, and thieves. Digital criminals are not currently perceived to be the broadest and largest set of illicit actors, either in local settings or transnational networks. In 2020, they may very well be, demanding a massive shift in the priorities of law enforcement.
3. **A lot hinges on how the political economy of data evolves.** In some scenarios, it is security issues around data—more than the security of digital devices or communications networks per se—that drive outcomes. When data becomes more easily exchangeable, it also becomes something of measurable value that criminals want to acquire and sell. The interactive dance between data and algorithms—where the scarce resource lies at any moment, where differential insights can be created, and where the most dangerous manipulations can occur—becomes an important variable in the shape of the threat landscape.

4. **Device security rules.** Many new types of devices (and accompanying security systems) will be developed and deployed by 2020, by a very wide range of firms (small and large) around the globe, and from diverse economic sectors. Many of these new entrants will be poorly prepared and lacking incentives to ensure security. This presents a significant opportunity for governments and transnational organizations to act.

5. **Cybersecurity is at the threshold of profound psycho-social impact.** The internet has already had a massive impact on nearly every facet of human life, including psychology, sociability, and the economy. Cybersecurity issues have not, until now, had anything near that level of impact on most human beings. Cybersecurity for individuals has been a nuisance or an embarrassment, a financial toll, and a source of fear and worry—but not a fundamental risk that changes how we live. Cybersecurity is about to have this type of psychosocial impact. This arena will feel more like nuclear security did to the generation of Americans who lived through the crises of the 1950s: an ever-present existential threat that shadows human life and calls for massive global action. Corporations and governments may become able to predict individual human behavior and come to "know" us (not just what we buy or where we go) better than we know ourselves. Memories may become storable, searchable, shareable, and possibly changeable. Such advancements will go to the essence of what it means to be human, how we interact with one another, what freedom and fairness mean, and ultimately how we assess a feeling we call "security."

6. **Public-private partnerships are everywhere.** It should be surprising (and troubling) that this observation feels situated in the future, but many private-sector and public-sector actors still behave as though the other "side" is not critical to cybersecurity outcomes. This is a dysfunctional mindset, and it will become even more so in the future. Successfully forging public-private relationships will be a source of significant security advantages for cities, regions, countries, and beyond. And as these partnerships multiply and morph, it will become harder to distinguish between what a private actor is doing and what a government is doing to threaten or defend networks and data assets. The public vs. private distinction may matter considerably less in 2020 than it does today.

7. **There is no silver bullet in cybersecurity.** The ongoing and ever-increasing demand for features, performance, and extensions of digital capabilities expands to fill the space of what is technically possible (and often goes beyond it). This observation, in light of the vagaries of human behavior that accompany it, means that the digital realm will evolve very much like other "security" realms have always evolved in human affairs: with ever-changing vulnerabilities that can never fully be mastered. In other words, bad actors coevolve with good, and the meanings and identities of "good" and "bad" are never settled. Threats don't disappear; they change shape.
8. **Cybersecurity approaches the center of corporate and national strategies.** The risk of cyberthreats to firms is now as significant a force as the "normal" unknowns that keep CEOs up at night: unexpected shifts in customer behavior, economic crises, disruptive new competitors entering the market. For countries, cybersecurity will soon (if it isn't already) be on the same strategic plane as a major threatening nation-state or transnational actor with imperialist or revisionist ambitions. Firms and governments that come late to these recognitions will have to work very hard and fast to catch up..
9. **The developing world will play a significant role.** Whether developing-world actors become hackers, lead the way in adopting or creating technologies, use market fluctuations to jumpstart their data economies, or something else, developing economies and societies will likely drive the evolution of the cybersecurity environment as much as—or even more so than—they drive the internet overall.
10. **Don't count governments out.** The most important determinants of the cybersecurity environment in the near future will not be cyberwarfare per se, though preparations for and deterrence of major cyberconflicts will be one of the shapers of the environment. As a result, we do not expect cyberspace to be fully militarized in this timeframe. Our scenarios reflect the proposition that governments are major players regardless, and in some respects they are even more influential and directive of change over time in market- and technology-driven scenarios than their militaries

> might be in the event of cyberwar. While private-sector interests have dominated the internet agenda for nearly a generation, these scenarios suggests that governments in the future have the potential to play more significant—and possibly more constructive—roles than they do today.

Because scenarios are models, not predictions, no single scenario that we have described in this work, nor any single implication, will necessarily "come true." Cybersecurity in 2020 will likely include elements of all these scenarios, in some indeterminate mix. Whatever that mix will look like, this work helps to demonstrate that "cybersecurity" will be stretched and broadened far beyond its meaning at present.

The cybersecurity world of 2020 will still be talking about malware, firewalls, network security, and social engineering. But it will also be talking about personal memories, new distinctions between what is public and private, the power of prediction, faith in public institutions, the provision of public good, psychological stability, the division of labor between humans and machines, coercive power (both visible and invisible), what it means for a human-machine system to have "intention," and more.

That is a very different and much broader agenda for cybersecurity than we find today. These scenarios are both a reflection and outcome of this broader agenda, as well as an effort to drive others toward stretch mindsets that will enable re-perception of problems and opportunities. We are convinced that at the intersection of human beings and digital machines we will find the repository of people's greatest hopes and fears. That is why cybersecurity deserves the highest level of attention, research, imagination, and action.

Please share with us your reactions, insights, critiques, ideas, and questions. They are essential ingredients for shaping forward-looking research and policy agendas that universities, governments, firms, standards bodies, and other organizations should adopt as we seek to get just a little bit ahead of the future of cybersecurity.

CLTC

Center for Long-Term Cybersecurity

UC Berkeley

Center for Long-Term Cybersecurity

School of Information

University of California, Berkeley

102 South Hall #4600

Berkeley, CA 94720-4600

cltc.berkeley.edu

@cltcberkeley