INFERENTIAL FOCUS

BRIEFING

IF 3908 May 16, 2018

TRACKING AND BIOMETRIC TECHNOLOGIES:

MONITORING AND SURVEILLANCE BLUR DISTINCTION BETWEEN PUBLIC AND PRIVATE...BUT SO WHAT?

CONTEXT & DYNAMICS

Digital capabilities continue *to expand and grow more influential, and as a result, the digitized ability to monitor and surveil has expanded and grown as well. The tools of this increasingly powerful capacity include Tracking, Biometrics, Facial Recognition, Multiple Inputs and AI-Aided Monitoring. While such capabilities increasingly gain influence and use in China, where monitoring has been embedded in the culture for decades, the acceptance of these capabilities in the U.S. (so far) seems to represent a challenge to a long tradition of privacy. Yet little pushback has taken place. We have identified several contexts that are giving momentum to the spread of monitoring capabilities: Permeable Borders, the Great Restructuring, the New Autocrats and Digitally Trained Consumers. The advancement and spreading acceptance of monitoring and surveillance in the U.S. is another example of how digital technology is Creating Its Own Reality and challenging traditional ways of operating and thinking.*

IMPLICATIONS

- *Big Data and social databases become more valuable.*
- *Companies that provide tracking, monitoring and surveillance equipment and software become more profitable.*
- *Intelligence gathered through these technologies becomes a competitive advantage.*
- *A steady increase in nonhuman interaction in business and government furthers a personal feeling of isolation.*
- *Privacy issues move into the courts for resolution.*
- *Hacking of private files from institutions continues to expand, eventually costing banks and insurance companies more money.*
- *Services based on collected data become more personalized and effective.*
- *Services in the "sharing economy" deploy monitoring technologies to increase safety of users and assets.*

INFERENTIAL FOCUS

BRIEFING

IF 3908 May 16, 2018

Accepting the Once Unacceptable

New hardware, new software and an emerging cultural acceptance are reshaping society's relationship to surveillance. Whether the method uses artificial intelligence (AI), Big Data, sensor systems, biometrics (including facial recognition), smartphones, in-home messaging systems, in-store tracking or any other of the many ways to ascertain identity or monitor movements and changes, fewer and fewer details of an individual's everyday life elude some kind of tracking network. And such tracking seems to be drawing less and less pushback (see **inF 810** and **inF 811**).

Fewer and fewer details of an individual's everyday life elude some kind of tracking network.

While some might use these networks to increase their own security and some might deploy them to monitor the behavior of others, both uses are iterations of surveillance, and technology has steadily increased the ability to surveil. In a condition that parallels the story about a frog in increasingly hot water, humans, enamored of their own digital devices, seem to be increasingly indifferent to being watched or listened to, activities which in the past would have been seen as invasions of privacy. Moreover, many youth who have grown up surrounded by and comfortably ensconced in a world of digital devices hardly seem fazed by such invasions. Recent pushbacks against digital technology and social media in particular have raised flags that seem to express concerns for breaches of privacy. Yet digital capabilities are so broad, so immense and so widely used that any kind of successful pushback against invasions of privacy will seemingly represent more of a diversion than a disruption to the advancement of surveillance and monitoring (see **inThought**, **11/20/17**).

Some of those who do worry about expansions of monitoring capabilities think that companies are simply collecting too much information about consumers and holding that data for too long. Others think the government, by collecting data and monitoring movements, is delving too deeply into citizens' lives. Both kinds of worriers wonder just what the collectors of such information are doing with the data. When hackers purloined 143 million personal files from Equifax, many individuals wondered what information Equifax actually had on them and how they had acquired it (see **IF 3804**).

Citizen and consumer concerns seem to revolve around a lack of transparency about what is being collected, how it is being used and what an individual should get in return for his or her information being collected. That is, the issue seems to be more about the use and abuse of collected information and less about the fact that the information is being collected or that individuals are being watched in the first place. There are exceptions to that perspective – some want such tracking ended – but the era of extensive and ongoing monitoring seems to be moving steadily forward, assimilating itself deeper and deeper into the culture. How is that happening?

"I avoided the bank security cameras. It was the selfies I took during the robbery that did me in."

Tools of the Trade

Alibaba's Jack Ma has suggested that data are replacing oil as the driving force behind a growing economy. Essentially, Ma is seeking to monetize what his country has been collecting for decades: personal information. However, with digitization, the state and affiliated companies such as Alibaba have access to much more data than ever before about individuals – such as credit reports, police reports, purchases, driving as well as professional licenses, insurance claims and the like. Individual Chinese citizens will benefit or suffer from the country's massive data-collecting project – with Beijing issuing each citizen a "social credit" number, or score – depending on whether the data reveal a positive or negative message about the individual. With a higher score, individuals can access banking systems, purchase airline tickets, buy housing, enter university and take advantage of other benefits. Those with a lower score, not so much. Meanwhile, similar kinds of data in the hands of Alibaba enables the company to provide more personalized and convenient services to its customers (see **IF 3807**).

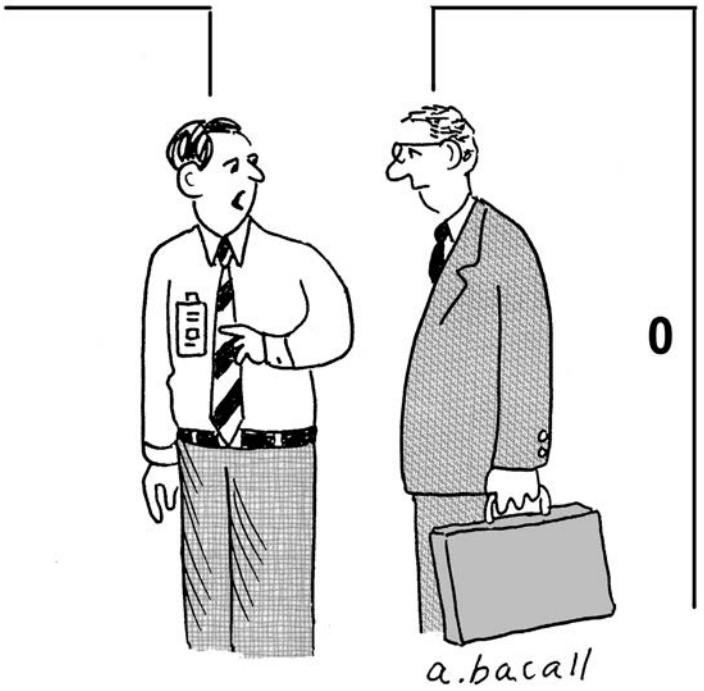
> The badge contains: a microphone to determine if employees are speaking to each other or on a phone call (and what they are saying); Bluetooth and infrared sensors to determine where the users are located; and an accelerometer to record the users' movements.

In Western societies, where there is a political tradition of privacy and where government surveillance has a checkered history, such monitoring has been viewed skeptically. Yet the assimilation of digital technology into mainstream activities – at work, in the laboratory, for the government, for interpersonal communications, for entertainment and gaming, and in all the many other places and ways digital technology infiltrates daily lives – has lessened more and more citizens' concerns about being monitored. Why is this happening? And just what are the tools of this more advanced ability to monitor citizens and consumers? First, the tools.

Tracking – The idea of tracking machines and environmental conditions has been used by industry for some time. For instance, railroad companies have implanted sensing devices on their rail lines and equipment to provide early warnings of possible problems before they create a crisis. Such tracking of business equipment morphed into wristbands and other self-monitoring systems that assist people doing physical workouts – keeping track of things like distance traveled, heartbeats and blood pressure. But recently, such tracking has started to turn toward monitoring others.

◆ Amazon recently won two patents for a wristband that can monitor what all shift workers are doing, vibrate if the wearer becomes idle and "decide" if the employee wearing the band has done something wrong. According to Amazon, haptic sensations passing through the device would help workers in their warehouses find the right bin faster. (*New York Times*, 2/1/18)

◆ A 12-square-mile neighborhood in Atlanta has installed cameras to monitor every car that uses the public streets in the neighborhood, using license-plate-identification software. Moreover, police had planned to store this information permanently, although a recent law passed by the state of Georgia limits such storage to 30 months. (*Atlanta Journal-Constitution*, 5/7/18)



"This biometric ID badge is part of the new security system. The badge contains my encoded retinal scan, fingerprints, and level of job enthusiasm."

◆ Humanyze provides Fortune 500 companies with ID badges the size of a credit card, with the thickness of a book of matches. The badge contains: a microphone to determine if employees are speaking to each other or on a phone call (and what they are saying); Bluetooth and infrared sensors to determine where the users are located; and an accelerometer to record the users' movements. Such badge data are then combined with data extracted from email and digital calendars to give the business owner a picture of how each employee spends his or her day. Other competitors for such employee monitoring capabilities include Hitachi, Workday, Microsoft and Veriator. (*Economist*, 3/28/18)

> "The days of having 40,000 to 60,000 people in the stadium and not knowing who they are, I think those days are going to disappear."

Autonomous cars depend heavily on such tracking technology to monitor cars, people and other objects that might enter into their pathway. Alarmingly, researchers at the University of South Carolina and at Qihoo 360, a Chinese security company, demonstrated that such devices can be hacked, making it possible for an outsider to trigger an accident. (*MIT Technology Review*, 12/17)

Biometrics – Most everyone might remember a movie or two in which authorities found their perpetrator by comparing fingerprints, the once surefire scientific (biometric) way to prove the guilt of a party. While fingerprints have faltered somewhat in authority because of some errors in their application, the field of biometrics has greatly expanded to include iris scanning, retinal assessment, body shape and scent, DNA, hand geometry and also facial recognition. These are physiological measures of an individual, and complement more traditional behavioral measurements such as tracking behavior as discussed earlier.

◆ Mastercard has started deploying biometric measurements, such as iris scans, fingerprints and facial recognition systems, to its authentication processes. Intended to provide better security and faster checkouts, such biometrics obviate the use of passwords, PINs or signatures. (*Pymnts*, 1/26/18)

Facial Recognition – Facial recognition technology is actually a biometric, but recent advances in its capabilities make it sufficiently important to warrant a category of its own. Facial recognition software is getting applied very widely and very quickly. Smartphones can now be switched on by facial recognition software, ATMs in China provide access to accounts via facial recognition software, a KFC restaurant in China enables customers to pay via facial recognition, and Beijing uses facial recognition software to add information to its citizens' files (*e.g.*, identifying jaywalkers and political protesters). Roughly 300,000 companies and individuals around the world have deployed facial recognition systems that use Megvii's Face++ software to monitor employees, visitors and outsiders. Hangzhou Hikvision Digital Technology, a Chinese manufacturer of security and surveillance equipment, said it would be producing 400 million surveillance cameras in the next two years to sell at home and abroad. Other security applications are being introduced regularly by companies such as SenseTime, NTechLab, Amazon, IBM and Microsoft. They all use databases stored in the cloud for image comparisons. China, because of its deeply deployed surveillance systems and also because of a greater focus on the technology by major companies, leads the U.S. and other developed economies in making and deploying facial recognition capabilities. Yet in the U.S., deployment is spreading. (*Washington Post*, 3/27/18; *Financial Times*, 3/23/18; *Economist*, 9/9/17; *Bloomberg*, 4/20/18)

◆ Madison Square Garden in New York City scans all who enter the arena with a facial recognition system to gain individual identification of entire audiences. Other American venues are experimenting with facial recognition. While this is intended to increase security, teams and bands playing in the arenas also gain more insight as to who attends their games and concerts. As one provider of such services to stadiums noted: "The days of having 40,000 to 60,000 people in the stadium and not knowing who they are, I think those days are going to disappear." (*New York Times*, 3/13/18)

◆ Despite overall challenges to funding, school districts from New York to Arkansas are installing facial recognition software to add security to their campuses. The systems include cameras posted inside and outside school, all of which are connected to facial recognition software that compares camera photos with images stored in the cloud. (*Gizmodo*, 3/16/18)

> "Australian company Westpac Banking Corporation is installing AI-enabled video cameras to identify the mood of staff members and to inform managers if they need to take some kind of mitigating action."

◆ Jet Blue and American Airlines have taken initial steps to install facial recognition in their boarding process, with the intent of eliminating boarding passes. Uber is trying a system in India in which drivers post a photo of themselves on a site that then assures the company that the driver is a vetted driver and not an interloper. (*Economist*, 9/8/17)

Facial recognition, even as it is being deployed in many public arenas, still has vulnerabilities. Wearing glasses with certain markings can cause errors in recognition, and darker skins tend to create identification errors. A changed texture on the surface of an object can confuse the software and cause errors. And of course, basic make-up, beards and added facial disguises can trigger mistakes in identification. (*Digital Trends*, 11/2/17)

Multiple Inputs – One way to overcome the weaknesses in each of the biometric systems is to combine them into a wider monitoring method. Using several biometrics might lessen the potential error for any one of them. For instance, Evolv's system is being deployed for security in "soft targets" – that is, places where security is less intense than, say, airports. For facilities such as malls and train stations, Evolv executes a body scan in one one-hundredth of a second (taken of people walking by and not at a special security point), and it captures a facial image to forward to a security database. The combination identifies a person and reveals if he or she is carrying "materials of interest." (*Ringer*, 10/26/17)

◆ Clear is a private company selling passenger services at airports across the country. A passenger who pays a fee and lets the company take his or her fingerprints, iris scans and facial images and allows those stored items to identify him or her as the person on a boarding pass, can move to the front of security lines. (*Ringer*, 10/26/18)

◆ Rival Sports provides sports franchises with systems that can identify and follow ticketed customers. Those using the software require fans to buy tickets online and to post a photo of themselves before completing their purchase. Owners can then follow whether the tickets bought by the original fan are sold to another party, who also must post a photo when making a purchase. Those entering the arenas without a posted photo can be stopped for questioning. (*Recode*, 5/4/18)

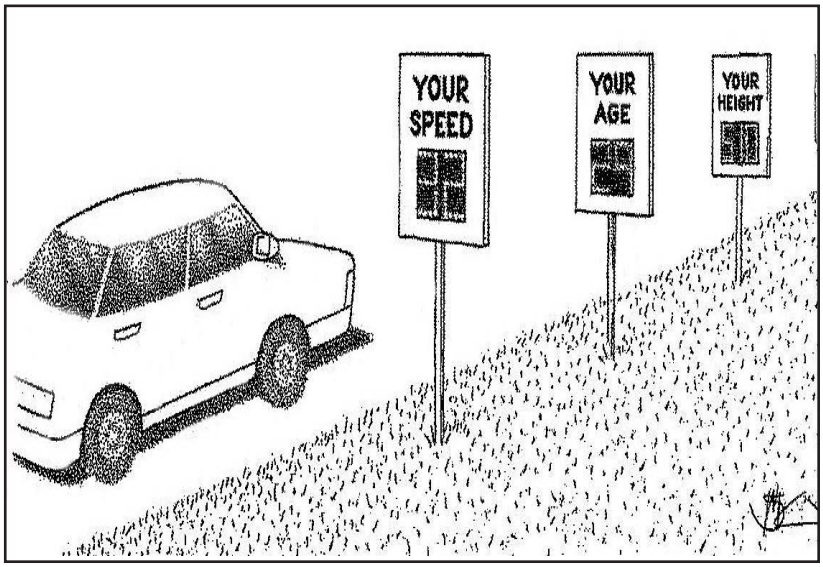
AI-Aided Monitoring – The Holy Grail of monitoring software involves the use of artificial intelligence (AI) to make "decisions" about the raw data that sensors, biometrics and other resources provide.

Surveillance in a Sweet Spot?

> New Autocrats seek to stabilize the disruption with promises of order, a signal that to them seems to call for increased surveillance.

Even as the foibles and biases of AI get worked out in labs around the world, it is, nonetheless, being deployed in airports and various surveillance systems. Facial recognition software, for instance, can include AI to make clearer connections between the person in front of a camera and an image located in a database in the cloud. But the AI link to surveillance and monitoring is already straining credulity.

◆ Australian company Westpac Banking Corporation is installing AI-enabled video cameras to identify the **mood** of staff members and to inform managers if they need to take some kind of mitigating action. Also, by exploiting AI's ability to "read" customers' faces and to connect to available financial data, the system can inform managers whether or not specific customers can actually repay loans they are requesting. (*Financial Review*, 11/14/17)



◆ 7-Eleven is rolling out AI-assisted facial recognition capabilities in 11,000 stores across Thailand. The system can supposedly identify loyal customers, analyze in-store traffic, monitor product levels on shelves, suggest additional products to customers and measure the emotional state of each customer. American company Remark Holdings is supplying the technology, which it has also provided to Alibaba, Tencent and Baidu in China. (*Business Insider*, 3/16/18)

Together, these various contributors to monitoring and surveillance services – Tracking, Biometrics, Facial Recognition, Multiple Inputs and AI-Aided Monitoring – have greatly advanced the capabilities of keeping track of people and things. Yet this steady advancement has received little pushback from the public in the U.S. Is that because Americans do not know monitoring and surveillance are happening, or that the new services are seen positively, or that individuals no longer worry about advancing digital capabilities in this area – or, ultimately, do they think it is too late and privacy has already been compromised?

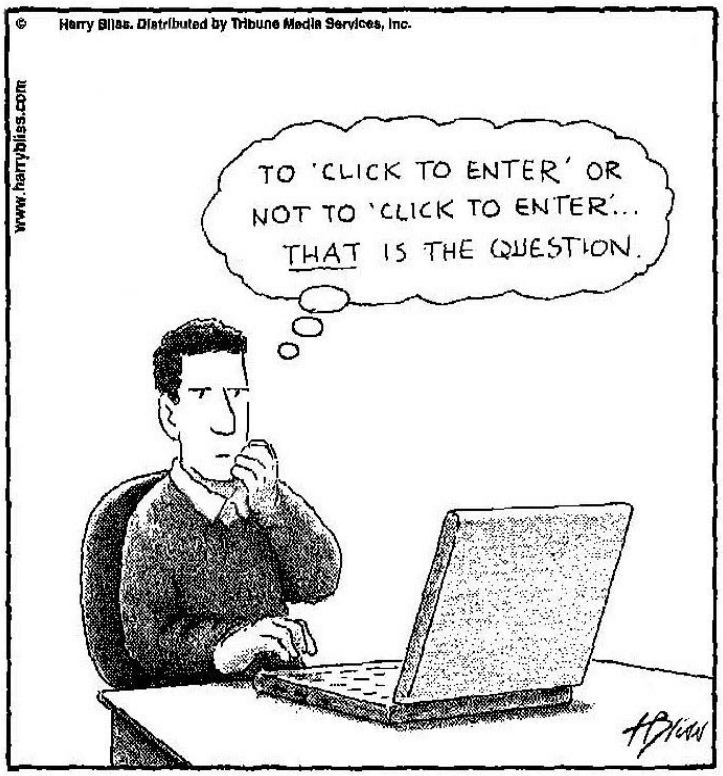
One reason such monitoring of individuals' behavior has moved ahead so steadily involves momentum gained from several social contexts we have identified. These contexts offer the parameters that seem to be allowing such challenges to traditional concepts of privacy take place over time.

Permeable Borders – When we first identified the three large changes moving across the world – the New Industrial Revolution (*a.k.a.* globalization), digitization and permeable borders – we suggested that together they were revolutionary forces. Permeable borders is the change that has triggered the most overt conflict in societies. People move across once clearly defined borders; religions, ideas and styles override cultural barriers; work and money can easily ignore national boundaries; new values transgress traditional values; new capabilities challenge traditional identities; and on and on. All of these are driving some people to reassert the past with walls, rules, nostalgia, and the like. The result: uncertainty, anxiety and a quest for stability, key drivers for increased security and monitoring (see **IF 2407** and **IF 2408**).

The Great Restructuring – The three large forces spreading across society cited above have forced changes in the way institutions operate and people live. Entire industries faced a daunting task: restructure the way they operated and thought to bring themselves into alignment with the new realities of globalization, digitization and, most of all, permeable borders. That brought seeming chaos first to the music and newspaper industries; then came retail, entertainment, branded products and so on. Permeable borders disrupted cultures and individuals; the Great Restructuring disrupted businesses and employees. Disruptions encourage collections of information, which means monitoring (see **IF 3324** and **IF 3905**).

The New Autocrats – So many disruptions and so much displacement further uncertainty and confusion, triggering widespread anxiety and worry. Individuals seeking stability and security made it easy for New Autocrats to reach leadership roles in governments. Autocrats seek control, and autocratic government leads to various levels of suppression, ranging from subtle forms of intimidation to overt clampdowns. This encouraged the need for monitoring devices. Whereas Permeable Borders and the Great Restructuring disrupted reality for most individuals, New Autocrats seek to stabilize the disruption with promises of order, a signal that to them seems to call for increased surveillance (see **IF 3602** and **IF 3801**).

Digitally Trained Consumer – A digital device in every individual's pocket has brought wondrous capabilities to the owners of those devices, whether that capability be interpersonal communications, shopping or buying, learning, viewing/listening or gaming. Falling in love with a device meant accepting all that it could do...including monitoring the owner's behavior. People signed permissions to the companies from whom they were granted access to those capabilities, and typically, they did not read those terms: in essence, individuals just wanted the capabilities. Over time, users became inured to the reciprocal aspect of those terms: being monitored. Winston Churchill once remarked: "We fashion the building and then the building fashions us." So it has been with digital devices, as surveillance and connectivity seem to align with each other (see **IF 3815**).



Creating Its Own Reality – Taken together, these challenges to traditional society have led to a different kind of reality, one derived from digital capabilities that undercut the dictates, behaviors and values of the predigital society. In the new reality, new dynamics have surfaced: security versus privacy; interpersonal communications versus monitored behavior; brick-and-mortar stores versus online "stores;" careers versus jobs (gig work); personal identity versus online identity; mass versus targeted; human control versus automated control; human learning versus deep learning; and so on – in short, a different reality, one that has individuals trying to perform at digital technology's pace, with many negative consequences, and that has business deploying digital technology in the name of efficiency-for-efficiency's sake. Efficiency and productivity encourage more and more monitoring (see **IF 3302**).

> Efficiency and productivity encourage more and more monitoring.

Some Pushback, But....

In such a reality, monitoring and surveillance become easier and easier to deploy and less and less difficult to get accepted. Acceptance in China is not up for grabs, as monitoring and surveillance are part of the political culture. And so, last year, China filed 530 applications for patents in the area of camera and video surveillance, and added another 900 applications for patents in the area of facial recognition, many times more than such patent applications from the U.S. (*Financial Times*, 3/23/18)

The most widespread focus on privacy has come from the European Union (EU), which passed the General Data Protection Regulation (GDPR).

Perhaps less emphasis on such patents in the U.S. and among other developed countries might result from a concern about legal problems over privacy issues. Yet in a country where individuals share their locations with Siri, their shopping lists with Alexa and their iris scans and fingerprints to get them through airport screening faster, the desire for privacy seems to be fading. In fact, according to a recent survey by the Annenberg School of Communications at the University of Pennsylvania, a majority of Americans "expect" to be monitored. And indeed, they **are** being monitored, as a recent revelation revealed: The National Security Agency (NSA) monitored more than 534 million phone calls in 2017, more than three times as many as it monitored in 2016. (*New York Times*, 5/2/18 and 5/5/18)

So far, only small signs of pushback among American institutions have surfaced:

◆ The Oakland (CA) City Council recently passed a strong privacy ordinance governing surveillance capabilities. Joining fellow California entities Berkeley, Davis and four other cities and counties, the council now requires an annual report from all relevant agencies on "how the surveillance technology was used" in the past year. (*Ars Technica*, 5/3/18)

◆ The ACLU and NAACP sent a joint letter to Arion, protesting the security-device company's newest offering: facial recognition software to all police departments. The letter cited the system's tendency to error when looking at dark-skinned humans. (*Washington Post*, 4/26/18)

◆ Citing a 90 percent error rate in field tests by police departments at music festivals in South Wales, UK regulators said that stronger rules governing use of such technology will need to be passed. (*Wired*, 5/3/18)

The most widespread focus on privacy has come from the European Union (EU), which passed the General Data Protection Regulation (GDPR). Taking effect May 28, 2018, GDPR says that personal data – anything that can identify a person, such as a name, address, etc. – and special categories of data – anything that can provide a bias, such as race, political opinion, etc.– are protected. Collectors of such data must inform individuals that they have such data and get permission from those individuals in order to retain that data. The fine for failure to follow the new EU rules can be four percent of global revenue. (*Spectrum*, 5/16; *New York Times*, 5/7/18)

Such new restrictions notwithstanding, movement toward wider and wider monitoring and surveillance in the U.S. and other developed countries is steadily advancing, and that is changing culture. The slow change revolving around privacy and its relation to monitoring is getting little resistance because of several culture shifts already underway, all brought about, in part, by digital technology. This significant change in yet another traditional cultural value is just one more example of digital technology, as we have written, creating its own reality.

"I'LL TELL YOU, ED, THIS NEW TECHNOLOGY IS STARTING TO REALLY SPOOK ME OUT."

Some of our previous looks at this topic:

IF 3905 From Work To Post-Work: Jobs, Work And The Ongoing Restructuring Of Employment, 3/29/18

inThought Digital On Defense: Negative Effects Of The Great Digital Experiment Challenge Silicon Valley, 11/20/17

IF 3815 Digital Technology Is Training Consumers: Consumers Think And Operate Differently, And Retailers Are Forced To Change, 7/20/17

IF 3807 China's Big Worry: Stability And Power Among Beijing's Leaders, 4/17/17

IF 3804 Systemic Surveillance: Watching Everyone, Everywhere - To What End?, 3/20/17

IF 3801 The New Autocrats And Their Increasing Appeal: Strongmen In An Era Of Instability, 1/5/17

IF 3602 The New Autocrats: Tactics Of The Early Twenty-First Century's "Chosen Ones", 1/26/15

inF 811 Sensing And Tracking Everything, Part Two: The Internet Of Things, 7/25/13

inF 810 Sensing And Tracking Everything, Part One: The People Will Be Watched, 7/24/13

IF 3324 The Great Restructuring: Society Moves Ahead In The Process Of Rethinking Everything, 11/21/12

IF 3302 Creating Its Own Reality: The Effects And Side Effects Of Society's Assimilation Of Digital Technology, 2/13/12

IF 2408 Permeable Borders And The American Psyche: Aggressiveness And Restraint In Contemporary Society, 3/31/03

IF 2407 World War III: Causing Increased Insecurity And Uncertainty, 3/27/03