Government, Private Industry, and Symbiotic Surveillance: Realigning 4th Amendment Challenge in Search Immersion Nation

Sam Guiberson

Washington DC - September 14th, 2017

National Association of Criminal Defense Lawyers

13th Annual White Collar Seminar

There are many laws of nature, but one immutable law of government surveillance is that every technology capable of a surveillance purpose will eventually be put to that purpose by government. Communications surveillance in America runs much deeper than a reluctant response to the urgent challenges of a post 9/11 terrorist threat. U.S. government surveillance has been robustly insinuated into communications technologies of the past whenever a sense of endangerment prevailed in the loftiest circles of national authority. Since at least World War I, government intelligence gatherers have been creative and resourceful in reaching for the boundaries of what was possible and permissible, even when it was not particularly lawful.[i] State surveillance has always been deployed in the shadow of popular technologies.

We must recognize that all corporate surveillance is ultimately also state surveillance, not only because the government can acquire commercial surveillance by process or payment, but because they mimic each others' behaviors in the voracious capture of our every digitally registered intention or recorded moment of screen attention. Surveillance capitalism[ii] and the surveillance state draw their parallel conclusions about us by methods of massive aggregation and computational analysis to translate collected data into either financial or intelligence assets.

While we have been assaying 4th amendment protections on judicial scales, weighing the measure of what privacies we will give up in trade for whatever law enforcement objective, promised security from terror, or personal convenience is dangled in front of us, surveillance technologies have saturated the entire bandwidth of human enterprise. The absence of aggressive 4th amendment challenges to this business model of industrial surveillance has only encouraged the evolution of a national industrial surveillance complex, in which our individual privacies are but commodities and our willing acceptance of such surveillance its commerce.

Lawyers, judges, and the public are not prescient enough to anticipate the wealth of surveillance opportunities and consequences that cascade from each new consumer technology, much less those cloaked in government secrecy. Because we are so technologically myopic, the contemporary boundaries of our expectation of privacy have been compromised in the courts because new technologies are analogized to earlier generations of technology thought to be comparable, rather than by assessing the potential risks of each new generation in the unique context of its deployment among other complex surveillance technologies.

So far, our modest barricades against these new industries of intrusion have surrendered us to a lifestyle of total surveillance immersion. 4th amendment advocates must now be as innovative as billionaire technologists in forging new disruptive arguments for digitally framed expectations of privacy. Not to do so ensures that an open ended exploitation of surveillance technologies will irrevocably disrupt the balance between the government's knowledge of its people's actions and the people's knowledge of how the government acts.

Because we have been lulled by the march of mundane technologies of only marginal privacy impact, we are unprepared to quarantine riskier technologies until we assess the long term consequences of their surveillance uses. If we fixate on the threat posed by individual technologies, it reduces the likelihood that we identify the multiplication of force achieved from the gathering of data streams that transcend individual surveillance devices. Whether they are digital, aerial, robotic, or voice capturing systems, their introduction into the petri dish of a technology-intensive society causes a systemic response that changes far more than

hardware. Our critical focus should on the congress of data and not the collection of data. When courts assess 4th amendment surveillance technologies by analogizing how each new onion skin is like the last onion skin, while ignoring the onion, aren't we making the wrong arguments?

Digital rights as bold as our Constitution require more than just putting a second scoop of analog thinking on the same 20th Century ice cream cone. To spin as fast as the digital engines propelling our society forward, constitutional arguments need to extrapolate from the technology we predict to what privacy we will demand. When American fighter pilots were first piloting the technological marvels that were jet fighters in the 1950s, they were instructed to put their attention 500 miles ahead of where they were to keep pace with the aircraft's astounding speed. To understand the tectonic scale of change that Internet enabled surveillance has brought to 4th amendment jurisprudence, we will have to think much farther ahead than that. It is time to stop pontificating about the promise of the Internet and start inspecting the Internet's plumbing.

_____

Technology is agnostic to the benefit and detriment of its uses. An inventor's idealism is easily exploited as her innovation matures and the multiplicity of its possible applications become apparent. The re-purposing of a modest technology into an exponentially more threatening surveillance system is not a factor our 4th amendment doctrines take into account.

It wasn't the invention of the cellphone that was the disruptive technology that altered the entire planet's relationship to government surveillance. The disruptive event was the miniaturization of cell phones that resulted in their universal adoption. Cell phones have

become such powerful tools of surveillance, not because they are hand held computers, but because they are in everyone's hands. It is not single data points but vast data sets that are taking the 4th amendment hostage.

No judicial litmus test of the 4th amendment "toxicity" of an emerging police surveillance technology occurs before each new wave of surveillance collection begins. Police department adoption of new surveillance products happens as fast as a hamburger disappears in a hungry dog's bowl, partly because the acquisition of new surveillance equipment is accelerated by private sector underwriting when the product's deployment presents a profit opportunity[iii]. While it is always Black Friday for police surveillance tech consumers, law enforcement's early adopter compulsion contrasts dramatically with what we do in other domains of innovation.

Consider the graduated adoption protocols for scientific advances in biomedical engineering and pharmaceuticals. We understand that their benefits, and possible risks of unknown consequences, must be subject to rigorous clinical trials before they enter mainstream commerce. We understand that biotechnology, medical, and pharmaceutical advances have such an impact on our collective well being that the public interest requires that they be subjected to a presumption of harm, absent scientific proof of a benefit far outweighing risks. The extent of our privacy risk analysis of a novel surveillance technology is to compare a peanut to a planet and agree they must be the same because they are both round. Analogizing a 1990 surveillance helicopter's impact on privacy to that of a miniature 2020 surveillance drone is tantamount to approving a new drug because it is dispensed in a pill similar to an aspirin. The holistic effects on the body politic should dictate the

constitutional consequence of technological change, not the constitution of a changing technology.

_____

As digital networks and digital enterprise became transnational, not only did defining controlling laws with national borders become more challenging, it opened surveillance opportunities for the congress of data by governments and malefactors all over the world. In the hands of technically sophisticated criminal syndicates, corporations, and intelligence agencies, the exploit potential of free range global surveillance is surveillance unbound by the restraints of the 4th amendment.

The modern police surveillance industrial network is as global as it is local. Cops are now customers in an international marketplace[iv], beholden to surveillance merchandisers promoting a vertically integrated complex of new surveillance tech and software. In this surveillance product smorgasbord, domestic and foreign government police first buy the collection devices and then are upsold to the new software systems that collect the collections.

Judicial review of a 4th amendment challenge to the police surveillance system du jour occurs closer to the point that the technology becomes obsolete than to its invention. The public and their defense lawyers have to play “hide and seek” with law enforcement and its surveillance industry enablers because they camouflage their next-gen surveillance tools behind a paramilitary mindset, rather than a crime prevention mentality. Despite the fact that a police cruiser parked at the side of a highway reduces speeding far more than an unmarked hot rod cop car doling out speeding tickets, law enforcement agencies strive to keep surveillance capabilities under the table. Not revealing legitimate surveillance capabilities

doesn't deter crime, it only deters politicians from second guessing appropriations and police conduct.

Law enforcement's sense of vulnerability isn't tactical, it's political. The more aware the public becomes of the scope of police observation of their private actions and activities, the more surveillance-antagonistic they are likely to become. Just as surveillance contractors justify non-disclosure of the technical specifications of their commercial products from defense counsel as corporate secrets[v], police departments and federal law enforcement agencies use the false front of court sanctioned protection of law enforcement's means and methods to conceal their addiction to citizen data collections and its cross-correlation with all other sources of state intelligence product. The prelude to a day of reckoning for the consequences of routine mass surveillance begins with outing the tools of surveillance, the hardware, software, and the algorithms that enhance data aggregation and meta-analysis.

_____

More than forty years into the Digital Era, we are still coming to terms with what digital privacy should be. Enhancing the classical definitions of a "person", a "place", "papers", and "effects" in digital experience requires us to articulate how the classical concepts of an expectation of privacy and the constitutionally grounded prerequisites for a "search" need to to change, or accept their irrelevance, because if we cannot define digital privacy, we will have no privacy at all.

The fault for our constitutional privacy predicament lies not with the courts, but with legal advocates' mistaking where the fault lines are in a vertically integrated surveillance immersion state. Because police surveillance is no longer a patrolman with a radar detector,

we cannot defend ourselves, our clients, or the constitution without redefining the fourth amendment in a way that the Internet can understand.

We are on the beaches of a digital Dunkirk. We are surrounded by an advancing array of superior technologies directed by highly disciplined operators committed to an all bandwidth assault. Our traditional assumptions about the established 4th amendment, protecting the person, the home, private possessions, and private communication have become an empty fortress, unable to defend privacy in the digital domain. How do we claim a 21st century stake in the 4th amendment while living in such a pervasive surveillance state? Here on our Dunkirk beachhead, we can't double down on anachronistic strategies that assailed simpler forms of surveillance technology. It will take thousands of small boats captained by creative lawyers, willing to cross some unfamiliar waters to reclaim the lost territories of personal privacy.

_____

The less hysterical we are about the next emergent technology being bent to the will of the surveillance state, the more strategic we can be in anticipating and then litigating the disruptive potential of its use. Privacy, like technology, is an ecosystem. Its preservation or degradation is the consequence of interwoven economic, industrial, and political progressions from the technological framework that existed before. For each new disruptive evolution of our advancing surveillance technologies, there is no such thing as stare decisis. In the coming era of 4th amendment challenges, we must first appreciate the very different physical laws of privacy in the digital century and then locate new pressure points that didn't exist in previous generations of less vertically integrated surveillance systems.

Until now, the 4th amendment has always been analog, standing guard over a world of Newtonian physics, in which a person, an object , one's property or documents was in one place or another, but not in many. The language of the 4th amendment confirms that the issuing of warrants depended on persons or things existing in three dimensions, "particularly describing the place to be searched, and the persons or things to be seized." No reasonable search could occur without particular specification, distinguishing the things to be seized from those that may not be seized, or from identical things that were in a different place altogether. Until the late 20th century, there was no ambiguity about the physical singularity of a person, a home, one's papers, or one's effects. Warrants were issued to search *a* body, *a* private area, pieces of actual paper and *a* property that was in one place only.

That concrete understanding of the person, place, papers, and effects is now buried deep beneath the soil of a post-digital world that is the love child of the Internet and quantum physics. All that the 4th amendment holds dear is no more certainly in any one location than Schrodinger's cat.[vi] Our personhood, property, privacy, and our papers exist only as scribbled electrons, found in one or many places simultaneously, stored in all sizes of physical matter with no moving parts, in which our secrets mingle indistinguishably among the grocery lists and summer photos of thousands of other people. What are our means of 4th amendment protection in digital space, when "digital space" is an earth-sized herd of electrons being driven like cattle by coding cow hands into stockyards of packets to be culled by math?

Whether our private pictures, poems, or journals of our marital problems are accessible to us in a sequence of megabytes stored in a hand held, computer held, or cloud held device should make no difference. Whether 4th amendment protection exists shouldn't be reduced to a question of the shape and location of our digital home storage unit, or its size, or its distance from us, or the diversity of its companion contents. What we hold private in the virtual world

is defined only by our expectations. What is reasonable about those expectations is not defined by antiquated judicial notions of what locations are suitable for keeping what is precious, but in the difference between how humans and machines perceive data. What privacy is in a digital society reducts to the Golden Rule – give unto others what privacy you would give to yourself. With that premise for what privacy is reasonable, no variance can exist in the 4th amendment protection afforded an elderly matron placing her heirloom necklace in her safety deposit box and a lonesome millennial storing PDF's of love letters on a distant rack of Amazon servers half a world away.

Particularity in the description of a thing to be searched for, in analog parlance, meant a specified, discrete object in a specified physical location. Digital searches of servers, smartphones, and hard drives treat the drive as the object, instead of the location in which the particular object of the search is to be found. That figure/ground reversal legitimizes general digital searches. Search warrants for computer servers, by today's standards, no more narrowly frame the scope of search to specified file content than would a warrant issued to search all legislators in the halls of Congress for a note in someone's pocket. Today, a single hard drive in a computer server harbors more diversity of content, privacy, and ownership than a Midwestern American city. Digital search warrants have undermined 4th amendment standards so grievously that law enforcement could search a digital Des Moines for an ounce of coke.

Some Things About The Internet of Things

The Internet of Things has but two critical components – the Internet and the Things. The "Thing" is a device with a thousand faces, ready to do the customer's bidding while also being busy with the biddings of its manufacturer. The "Internet" is the open line on which the

“Thing” calls up Corporate over Wi-Fi and dumps all that it knows about your looks, your house, your words, and your movements into an even larger digital netting that fuses “Thing data” into internal consumer marketing intelligence, or, more cynically put, into commercially strategic business intelligence products digitally sculpted from dubiously legal non-consensual searches.

Unlike old fashioned business relationships with customers where businesses focused on gaining profit from a transaction, in an Internet economy, ingenious, computer driven, mass data-analytical programs perform digital alchemy with the entire panorama of personal information collected from the customer. The donuts you order online generate less profit than the details about yourself you surrendered to buy them.

This is the business model known as Surveillance Capitalism. Driven by this model in which captured customer decisions, behaviors, and communications are cash cows, private sector surveillance leads us into uncharted waters in which law enforcement’s interests are barely submerged. If a powerful and resourceful technology sector continues to fixate on possessing our every privacy as its profit center, the “Internet of Things” and most every other digital thing, will continue to fill a bottomless well of personal information that will forever irrigate the government’s crop of citizen surveillance databases.

The most practical means of defending privacy is to recognize the next privacy attack before it is implemented. Because profitable business is the goal of private sector spying, turning your lead into their gold, the first defense of privacy is to preemptively decline to deliver the lead. The battle to restore the 4th Amendment may well begin in an online store, rather than in a courtroom.

Public disclosure of the surveillance capabilities of a website, a software, or a consumer product discourages consumers from doing business. Consumers want to preserve their privacy. There are ready examples of this fact in the explosion of end-to-end[vii] encryption messaging software products and anonymizing web services in the wake of the Snowden revelations. Just as there is reluctance in the law enforcement community to advertise their surveillance capabilities, so it is in the private sector, where the outed "spy product" disguised as a household appliance gains little market share. In response to public outcry and self-interest, the Internet's titans of industry stoutly defend your right to keep your communications with others private, just not your communications with them.

We can achieve a small measure of surveillance salvation through attrition. When a company can't get its product into the consumer's home, the government is deprived of the opportunity to eventually extract any captured privacies from it. Publicizing potential consumer privacy threats may not seem like a criminal defense litigator's forte, but lawyers' awareness of these types of surveillance capabilities enable us to explore prosecution reliance on such evidence in court. The defense bar's continuing legal education is to know what household and Internet consumer surveillance exists in the marketplace where law enforcement goes shopping every day. Trying to fly that 500 miles ahead of the demands of today's issues to litigate tomorrow's requires criminal defense lawyers to carefully inspect all the fine print that guides the lopsided, symbiotic relationship between a digital product and its end user.

_____

When the local police or federal agents hear bells telling them they should search your client's house, how much better would it be if the police could obtain a detailed floor plan of

your client's home from the company who sold him a robot vacuum cleaner? This is not a speculation about the future. It is an example from the present.

In a recent article in The Guardian,[viii] iRobot's Chief Executive offered that his company "may begin selling the floor plans of customer's homes derived from the movement data" of the company's Roomba robotic vacuum cleaner. The CEO advised the reporter that some Roomba models generate a digital map of the floor plan of its customers' homes, ostensibly to guide Roomba most efficiently into every room's nooks and crannies. To do so, it uses laser sensors, short-range infrared, and a camera with a cockroach's eye view of your home. Raw data from these components is organized by device software into something termed "simultaneous localization and mapping". This technology is known by its acronym, "SLAM", drawn, no doubt, from the acronym rich labeling environment of the U.S. military, where iRobot cut its corporate baby teeth making battlefield robots[ix].

If more proof is needed about the tech sector's enthusiasm for owning every last byte of your privacy, one industry observer called the proposed home map "a tremendous first-mover advantage" and, throwing some shade on the rest of the vacuum industry, said that "The competition is focused on making cleaning products, not a mapping robot." Note that the smart money is now on building household appliances that are only disguises for surveillance collection. So much for the prospect of corporate self-restraint in purloining intimate details from your private life for sale to the highest bidder.

It took only three days of viral news coverage of this new marketing idea from iRobot for public & tech media outcry to force a hasty corporate retreat into "never" land. The same executive issued a statement claiming that the company was misunderstood, and will never sell the Roomba location mapping to third parties, like Apple, Google, and Amazon[x]. No sale,

however, does not mean no law enforcement access, if floor mapping surveillance data is just another business record.

It is crude and ill informed to describe the Roomba-to-iRobot home surveillance data feed as only a business record. It is actually a transmission, an ongoing conversation between Roomba Model 980, serial number T4399A8F, owned by John and Leslie Harold, of 3562 Pine Shore Drive[xi], and iRobot's servers, constantly updating the map of its premises every time it does a housework chore. It is a lot to keep track of for a little robot, but luckily, its forever home has a strong Wi-Fi signal that allows the Roomba to pass along all that measuring data and that little camera feed to iRobot's corporate servers. Police could obtain access to this stream of data in real time, to be sure that the suspicious backpack under the Harold's dining room table that Roomba keeps running into doesn't move.

The most surprising 4th amendment risks are these "hi-tech bait and data snatch" private information collection systems that are so novel that the defense bar has no framework in precedent to assess them, beyond the intuitive, felt principles of violated privacy. Many of iRobot's 17 million Roomba floor cleaners are gathering and updating data about every interior detail of each of their owner's home layout, how it is furnished, which rooms remain off limits to vacuum cleaners, and every other feature of the interior floor space. Any firearms leaning against a wall? A lock box under the bed? A shotgun? Where does their Pit Bull like to nap? All Roomba-ready for law enforcement, all good Intel for when a no-knock entry is the order of the day. The "Internet of Things" is more aptly named the "Internet of Things Soon To Be Searched."

Internet of Things surveillance, and other similar personal data collection schemes in the "Internet of Websites," may allow 4th amendment advocates unexpected openings to set

limits on the 3rd Party Doctrine's applicability to platforms of Surveillance Capitalism. The cracking that nut requires defense lawyers to differentiate the founding premise of the 3rd Party Doctrine from the founding premises of this alternative business model.

Every lawyer knows that the 3rd party doctrine was born in a pile of Mitch Miller's records at his local bank[xii]. In the Supreme Court's judgment, Mitch's "consent" to the surrender of his 4th amendment rights to his financial records was established by his election to enter into a business relationship with his bank. The type of relationship that bank customers enter into is an exchange for specific services in return for a set fee. Choosing to "bank" required a voluntary surrender of the customer's private financial information because the bank's control of those records was essential to the performance of services for which the bank was being compensated. Providing the banking services to a customer depended, for the benefit of both parties, on the preservation of records about funds on account, funds dispensed and credited. The business records in question were for the sole purpose of the business relationship, recognized by each party to be the entire scope of their agreement for services performed for the customer and the bank's compensation for serving the customer.

From the factual premise for the United States v. Miller decision, neither Mr. Miller, his bank, or the Supreme Court majority, could imagine a future in which a service or a product was designed and built to profit, not only from the services their customers' chose, but from an exploitation of the information provided and generated by the customer, about which the customer would know nothing and from which the customer could expect nothing. While Mr. Miller lived in a world where bank customers expected banks to keep their money on account, modern day Internet entrepreneurs foist a two layered relationship on their customers, one for which they keep accounts, and one for which they do not have to account.

If the 3rd Party Doctrine exempts the bank customer's confidential data from 4th amendment protections because consent is implied by the customer paying a bank to perform the known services of a banking business, how could that consent extend to a separate, undisclosed and secret business of profiting off the collection, manipulation, and sale of otherwise 4th amendment protected personal data, entirely outside the scope of the business of banking? The line of court precedent establishing the Third Party Doctrine always relied on the fact that the customer knew what business the 3rd party was in, as that customer surrendered exclusive control over personal information.

When a customer purchases a Roomba robot to vacuum her apartment, money is paid for a computerized, self-navigating vacuum cleaner, not for the remote hoarding of a data stream intimately mapping the interior of Apartment 5G. In the software industry, consent is defined by acceptance of the terms of license in the product's EULA (end user licensing agreement.) No acceptance of the EULA, no robot software for you. When agreeing to Roomba's EULA, the customer is conditioned by her experience with retail purchases to believe that she is buying a robot vacuum cleaner that sucks up carpet dust, not one that sucks up a map of her house and the fit of her possessions within it in the act of doing its vacuuming duties. Since software and hardware technology companies have started playing this kind of two card Monte with their customers, and with 4th amendment law's notion of consent, we are likely on the verge of asking courts to review the customer EULA's as closely as 4th amendment case precedent.

For example, the Roomba's EULA reads in part:

> *The Product Software may cause the Product to automatically communicate with the iRobot's servers to deliver the functionality*

described in the Product Guide, to record usage metrics and to collect personal information as described in the iRobot's Privacy Policy. *(emphasis added)*

Okay, lets look at the Privacy Policy…

PRIVACY POLICY - Some of our Robots are equipped with smart technology which allows the Robots to transmit data wirelessly to the Service. For example, the Robot could collect and transmit information about the Robot's function and use statistics, such as battery life and health, number of missions, the device identifier, and location mapping. *(emphasis added)*

Does the skillfully lawyer-crafted ambiguity of the term "location mapping", added after that serial listing of data only a service technician could love, inform the purchasers that Roomba is mapping and transmitting not only *its own* location in your *house*, but mapping your *entire house?* Does such a faux disclosure of actual intentions meet the standards of consent in a relationship with a 3rd party business, such that it defeats their customers' right to privacy in their homes? The fact that these reporting functions can be turned off by the technically adept consumer[xiii] demonstrates that they are not at all essential to vacuuming functionality.

The foundation of the Third Party exception rests upon the customer's surrender of his privacy in a business transaction with a 3rd Party only insofar as that surrender is necessitated by the scope of services being rendered. No bank can sneak into your bedroom and search for the location of a steel safe beside your bed stand, and then provide the location to police

authorities on request, because it is in the business of protecting your deposited cash on account. The entire structure of the third party records exception is built upon the premise that personal information provided to, or generated by, a 3rd party is that the business records are only an artifact of the course of the performance of the business service the customer fully understood and consented to.

How do we craft an exception to the third party exception, disallowing warrantless law enforcement access to all personal data collection not obtained specifically for a purchased product or service to function? Such an exception would do little to curtail the commercialization of customers' privacy, if consumers choose to be promiscuous with their consent, but it would do much to prevent the exploitation of such consent by law enforcement. If defense lawyers don't aggressively challenge corporate collection and law enforcement access to the fruits of the poisonous robots, technology companies will continue to make the "Internet of Things" a water well of collected privacies that never runs dry, brimming with customer surveillance for law enforcement to quench its thirst.

_____

The iRobot case study is not a condemnation of a modest, if pricey, household robot. Roomba is but a bottom tier component, deployed to perform a function that creates an opportunity for data collection about its user. In this way, other than its talent for lifting pet hair out of carpets, it is really no different than a commercial website.

Like Roomba, the entire business model of web commerce is based upon the collection of consumers' choices made in the course of enjoying the appliance, product, or web platform provided them. Those choices can be what users buy, what web page users look at, for how

long, what patterns of interest the user shows in sites visited, etc. That data is then combined with that customer's past order profile, public information, and demographics to transform raw data sets into an asset that calculates individual and collective customer tendencies. Whether that "customer" is a homemaker, or a terror suspect, makes little difference to the digital machinery, and all the difference to the government's criminal intelligence consumers. It will take a much stronger spine in the digital 4th amendment to trust that the government can tell one from the other.

We have come to accept that our cellphone signals can be used to find us on a map, or our Internet Protocol number to find us on the Web. What is most destructive in 4th amendment terms, is neither the momentary digital captures of our longitude and latitude that fix our whereabouts, or even the web track that identifies our "thought abouts." It is the relentless capture of our habitude, the entire narrative of our physical and digital interactions fused into a mosaic of our manner, movement, and customs over time. It is those patterns in the full physical and digital spectrum of our personal behaviors that are most at risk, as our privacy interests in both physical and digital space degrade. The search for our habitudes is the Holy Grail of digital surveillance, because a person entirely watched is entirely understood, and a person who is entirely understood is the captive of those who are watching.

This is the steady glaze of a surveillance capitalist enterprise. It relies upon a hierarchy of integrated technologies to accomplish a progression of surveillance objectives in a permissive marketplace and political environment that sanctions surveillance by default. The end result of systemic surveillance is an intelligence asset, a surveillance meta-product that is predictive of future relationships with customers, competitors, enemies, and political adversaries. The ultimate functionality for these meta-intelligence assets is the opportunity they present for whatever political, commercial, or espionage advantage is to be gained from

placing bets in any poker game in which only your computers can model how future cards will fall. Surveillance capitalism treats your surveillance as its poker chips, but will entertain selling them to our government and to other governments as well.

_____

Internet and digital technological innovation is rife with unintended consequences that expose utopian intentions to Machiavellian subjugation. The architecture of the global, digital inter-network is such that the memory of all traffic passing within it can be stored until deleted. Mass storage advancements have made feasible the universal capture of the patterns of our movements, our choices, our purchases, our political expression, our vocabularies, and even the discrete idiosyncrasies of our facial features and speech. In digital capture, there is no practical limitation upon surveillance scale. The many become as easily followed as the few. The Achilles heal of our classical privacy expectations is that the growing threat of universal and perpetual capture of our digital personhood will constrict the liberty of thought and fearless protest that our Constitution was meant to protect.

_____

Still another dimension of how Surveillance Capitalism's profit motivated engineering of the digital marketplace exploits privacy and promotes state surveillance is the new voice activated intelligent personal assistant product category. These devices like Amazon's Echo, Google's Home, and Microsoft's Invoke evolved from smartphone and laptop speech recognition applications that turned voice commands into action steps within voice enabled applications. What putting that same functionality into a table top device has done is broaden the range of interactions the consumer and the device can accomplish together.

Each of these devices is a profitable token deployed among consumers to perform as a field research lab for proprietary natural language processing and artificial intelligence engineering. The objective is to develop an artificial intelligence that fluently converses and responds to humans. Each customer's small talk with his home assistant helps the company perfect natural language human-to-computer communications software that would allow digital simulation of human conversation. The resulting conversational computing systems would move out of the labs and into the world as universally effective surrogates for human command of both physical and digital machines. A truly conversational human/machine interface would disrupt computing technology like no other application has to date. Imagine Kubrick's HAL on your nightstand, with an equally hidden agenda.

Building a global community of hundreds of thousands of people simultaneously running their own test beds for Amazon's AI research department would be a dream come true for that technology company or any other. The value is not merely in the refinements Amazon can make to its voice recognition and emulation programs. It is in the fact that the more we communicate with computers, the faster they learn how to use our language to reason with us.

How could using such a convenient little digital appliance offend constitutional interests? The illusion involved is that this unassuming little box for which the customer pays good money is just another IoT "Thing" that the customer interacts with. The home assistant "Thing", when activated by a word it hears while constantly listening to the ambient sounds and conversation in the home, immediately engages with its master server for its AI software to interpret the odd communications mode that humans employ into something computers can work with. Once the server has solved that translation problem the best it can, it directs

commands back to the box sitting on your end table to comply with either your vocal directive to turn on your smart dishwasher or lock the smart door, or perhaps explain to you how light gets stuck inside a Black Hole. To add that disarming level of humor and familiarity that humans enjoy, it may also respond cleverly to thousands of off beat queries drawn from pop culture, politics, and relationship advice, based on company technicians' senses of humor and customer feedback.

It is a relatively low bar for law enforcement to obtain warrant access to the device to alter the active listening mode initiation that uses a word like "Siri" to an always on voice activation mode, similar to what hand held voice recorders do. Law enforcement using Echo like a Title III surveillance bug is no alarming paradigm shift in surveillance capabilities. IoT "things" become more constitutionally dangerous when the stream of voice interactions can be preserved as a "business record." Unlike Roomba, the functionality that was promised to the customer at point of sale is dependent upon the feedback loop of data being exchanged with an Amazon server hiding in some cloud.

Just like the Roomba, the "things" named Echo, Invoke, or Home seize value in the interactions with its multitude of customers that are integral to the service it performs. These interactions, similar to what websites do with users' clicks, can be monetized by feeding back products, services, or vacation spots its customers verbally express interest in, or pass this future marketing info along to "service partners" who follow up with targeted offers to the customers. Preserving such valuable marketing data from the customer's own mouth isn't so valuable if it is merely noted in passing. Surveillance capitalism craves customer data preservation so that it can digest the data retrospectively to model future individual and group consumer tendencies and consumer behavior, as their proprietary algorithms gain more

experience with your speech patterns and thought patterns. Of course, law enforcement agencies archive wiretap and undercover recordings, but they are passively listening to those conversations, not machines making conversation.

We have grown accustomed to customer data collection about our web usage, but will the public perceive an uncomfortable threshold in the surrender of large volumes of their personal voice samples and communication habits, even if the conversations are only with a highly responsive computer network that has a tabletop foothold in their living rooms? So far, the technology of such products may seem more like high touch sales technology than surveillance technology, since the customer consents to using his voice to enable the product and understands the product is performing as expected by using the customer's voice as data entry. The Internet generation seems comfortable with having their personal information used for marketing purposes, so there is likely to be no friction with that aspect of the bargain and the 4th amendment's standard of reasonable expectation of privacy. As with the Roomba, the confrontation with the 4th amendment doesn't come within the confines of the service provided, but with the manufacturer's exploitation of the customer's conversation data to fulfill a completely different corporate ambition.

As with questions about Roomba, do customers consent to the degree of voice sampling and discourse retention that devices like Echo are capable of? More importantly, are customers adequately informed of, or could they even imagine, the prospect of the use of their communications for such esoteric research and development? Are they consenting to use such devices with knowledge of how the users' content will be exploited far into the future? When clicking "I agree" on that licensing agreement, is that the service the customer

thinks the business is conducting with him? The underpinnings of the Third Party Doctrine depend on how those questions are answered.

To demonstrate the level of disclosure common to the End User Licensing Agreements in this market sector, this is what consumers must agree to the terms of service that, for Amazon's Echo, read as follows:

> *Your messages, communications requests (e.g., "Alexa, call Mom"), and related interactions are "Alexa Interactions," as described in the Alexa Terms of Use. Amazon processes and retains your Alexa Interactions and related information in the cloud in order to respond to your requests (e.g., "Send a message to Mom"), to provide additional functionality (e.g., speech to text transcription and vice versa), and to improve our services. We also store your messages in the cloud so that they're available on your Amazon Alexa App, Amazon Echo, Echo Dot, and Echo Show.* (terms as of June 23rd, 2017: underline emphasis added)

There is no disclosure of the duration of retention or specificity as to what "services" personal voice exemplars are applied to improve. Do they include the conversation's content, the topics referenced, or the conversational patterns of human request and digital response? Does a naive, blanket acceptance of an unlimited term of retention and exploitation for unknown corporate purposes establish an informed consent from the customer? In recent years, courts have become more sensitive to the duration of law enforcement surveillance encounters and explored whether 4th amendment standards extend to the protection of citizens' habitude in their personal patterns of travel over an extended period of time.[xiv] While these are important issues to resolve in favor of surveillance limitations, they don't speak to the question of whether long term retention and data analytical processing of conversations and voice samples held in corporate hands can be denied to law enforcement as business records.

It may be making some elements in government envious that the tech industry is liberally sanctioned by means of nebulous terms and licensing disclosures to use such data at will. Although 4th amendment protection does not extend to private actors engaging in the private enterprise of data collection, the social damage being done by the unforced servitude of personal privacy to the surveillance initiatives of the technology industry justifies reconsideration of the unrestricted agency of private actors to collect personal data, and then provision that personal data to law enforcement, whether by consent, compensation, or by means of the Third Party Doctrine.

The massive digital archives that store a compendium of our conversational exchanges with home assistant devices stockpile the raw material, the data capital, needed to conduct a world changing experiment with staggering surveillance potential. Over time, with continuing customer input, not only can the makers of these products perfect the ability to communicate as you would with your own spoken language, but to use your own spoken language to speak like you. With your volunteered conversations, the most ambitious prospectors in the voice mining industry want more than perfect transcription or translation of your words. The trend of their innovation suggests that the industry hopes to go beyond performing services the customer speaks, but to have its computer systems speak independently as the AI software has learned the customer would. There is money in expropriating your personhood to create your linguistic avatar.

Such systems as these have enormous commercial and surveillance value. Such a technical capacity to listen, comprehend, and appropriately respond to many individuals

voices can be sold to lesser barons of industry who don't have the requisite technologies to create such tools themselves. Companies could make robocalls to their customers where the pleasant and conversational robot you are talking with seems to know more about you than you do. It might be possible to sell to our government, or another, the ability to understand the voice communications of an entire population and to aggregate the data from all their communications, using software to infer their intentions, politics, and social networks in a specific geographical area[xv] such as California or Ukraine, depending on your government customer's tastes.

One might expect all surveillance disposed governments to have this tech all worked out for themselves. Governments are constantly surveilling conversations somewhere and know all too well how to copiously record them. What governments cannot create with their R&D, that a conversational widget maker can, is voice-to-computer exchanges with willing and unwitting customers whose lack of awareness of being recorded avoids the bias of self-consciousness. The randomness of millions of such two party exchanges between a person and a computer educates corporate AI systems to continually enhance their skills of spoken language-dialog, and then use the data from these conversational experiments to accurately interpret not just the meaning of words, but the customer's mentality. Massive sampling of interactive communication provides feedback on the AI machine's efforts to draw meaning, content, and predictions from patterns of conversational topics. In short, governments can't crowdsource[xvi] their research about wiretapping the world the way private enterprise can by using surveillance as a customer service. For this reason, governments will have to pay for, or purloin, such assets from the Surveillance Capitalists.

There is law enforcement application for such technologies in a much smaller scale than bugging the world. The technical capacity to simulate conversation speech and to process semantically appropriate responses in real time, to communicate as humans do, opens up a new domain for policing; using voice simulations as police investigators. Consider how budget friendly automated police investigation could become if digital voice avatars capable of conversing with suspects over text, email, or telephone could simulate undercover police officers in sting investigations.

In a few years, if a bulked up Echo is able to conduct a conversation with all the conversational attributes and tonal constructs of informal human speech, and engage in a conversation about whether you want to call an Uber or a Lyft, couldn't law enforcement use the same software tech to make undercover calls to suspected jewel thieves and engage them in telephone conversations about fencing the goods with fence-to-thief repartee garnered from thousands of similar conversations? Such robotic undercover operators could use mass computer analysis of all such prior recorded calls to code subroutines[xvii] that generate a rapport with a suspect, just as consumer robocalls now try to simulate casual conversation to entice a response from a real person to a robocaller that the real person momentarily perceives to also be a real person.

There are also police investigations and police intelligence operations that could evolve from AI human simulation software to assume the voice identity of one specific individual. Creating a large enough sampling to transform a laptop speech software package into the familiar voice of a gang leader would draw upon a sampling of perhaps a twenty hours or less of his wiretapped conversations. Once the computer program had learned the topics and conversational patterns of the conspiracy in progress, how very helpful it would be to record

evidence against co-conspirators, if the authentically reproduced voice of the boss of the conspiracy made calls to his minions and convincingly conveyed his instructions for their next act in furtherance of the conspiracy? With the flip of a switch, instead of the flip of a criminal boss, recorded evidence could be obtained with little human police effort. Drawing from Star Trek lore, these AI driven investigative techniques would begin the transition from a "carbon based unit" working undercover investigations to a "silicon based unit" making cases from the insides of a police computer server.

_____

At this stage in the hypothetical evolution of AI law enforcement, all the fruits of years of research in surveillance technologies, mass aggregation, and data analytics make the final turn. Surveillance automation will inevitably begin a transition from computing machines acquiring human traits to bringing its digital machinations of virtualized human behaviors to the real streets. Today, those streets are the streets of Dubai.

The headline of an article published on *The Verge*[xviii], reads "Police in Dubai have recruited a self driving robo-car that can scan for undesirables." This article describes a mobile surveillance unit with a 360 degree camera that "scans for wanted criminals and undesirables." Major General Abdullah Khalifa Al Marri of the Dubai Police Force, is quoted as saying: "We seek to augment operations with the help of technology such as robots. Essentially, we aim for streets to be safe and peaceful even without heavy police patrol." As a surveillance cherry on top, the O-R3 features an on-board drone to follow individuals to places the bot can't go. The Dubai police department wants 25% of its police force to be robots by 2030.

The O-R3, in the configuration described in the article, is little more than a telepresence machine[xix], providing a roving video feed supplied to officers comfortably seated in their cubicles back at Dubai police headquarters. Like many other robots now roaming robotic labs all over the planet, O-R3 strives to accomplish one or many human activities in the way that humans do. At this relatively primitive stage of robotic development, much is made of successful human motion and task simulation. Here, the O-R3 is just a set of wheeled eyeballs walking the beat, a sort of Roomba with a badge, but with bigger wheels and a camera[xx]. The hint of what is to come is hinted at in the article's reference to "scanning for undesirables".

What O-R3's anticipated use of facial recognition technology reveals is that it has the same type of sustained Wi-Fi feed to an intelligent server as do Roomba and Echo, running 24/7 somewhere in the cop cloud. Like the Echo, the O-R3 is but an extension of a much more sophisticated, complex hierarchy of software and technology than meets the eye. We have learned from contemplating the hidden surveillance objectives that are concealed within modest devices like home appliances and home assistants that they are but pleasant pawns in a larger game of commercial surveillance and research & development. OR-3, in one iteration or another, will gradually broaden the bandwidth of its actionable intelligence in the field to access, and then respond to, the grand scale of all the private information profiling data and analytics that the technology industry and federal and state law enforcement have constructed.

As a future version rolls around the streets like a robotic riding lawn mower, it makes decisions as a human officer's surrogate, drawing from a data field larger than the combined

police experience of all law enforcement officers who walked its beat before it. As it communicates with its server, and receives instructions from it, it gathers electronic signals, facial images, and conversation it passes by. As it goes, wherever it goes, it O-R3 is tirelessly adding to that invisible archive of all data the surveillance system combines from all its receptors in order to inform them about us. All we have struggled to teach computing devices, all that we have innovated to help them imitate us, all that geniuses have created to teach them to speak human language, predict our behaviors and act in our stead, now comes full circle to the era in which our digital machines will act upon us. No doubt, there are many ways in which robotic devices will act with humanity, but they mirror us too well to be incapable of our inhumanity. It will be in the code.

This will be not only the forensic study of code, but an exploration into how due process varies from data process. We have to compel the modern surveillance systems that act upon us as police surrogates to pass the Turing Test, the renowned British computer scientist's method of a machine's ability to behave intelligently in a way equivalent to, or indistinguishable from, a human being[xxi]. How courts discriminate human conduct from the digital emulation of human conduct will depend on how vigorously we defend the principle of the peoples' right to control all the artifacts of their humanity as they are described in the 4th amendment, no matter whether they exist in a person's physical or digital experience. The integrity of 4th amendment standards may depend on whether courts will hold law enforcement to account for using the stolen parts of our privacy to build the surveillance machines.

Our legal challenge is to differentiate probable cause from probabilistic cause; the one being a human judgment and the other a computer simulation. The current trend[xxii] towards

the substitution of machine judgments for human judgments is predicated upon the statistical assumption that data analytics can offer a substitute for human decision making, that data driven probabilities are the same as what people think probable. No mater how economically efficient the substitution of pattern recognition for human opinions will become, emulation systems do not substitute for human judgments because, for better or worse, they do not see the data as humans do. Justice rendered by AI data is driven by comparing outcomes; human justice, by the fairness of process. To defend against computed conclusions, we must relentlessly attack each computer instruction upon which the next computer instruction relied. Just as we have learned that you can cross examine a tape recording, we can learn to cross examine what computers have learned from recording us. We lawyers now have so much to learn because there is so much to lose.

i For an account of US surveillance practices from the 1st WW to the formation of the OSS in the 2nd WW, See James Bamford's book The Puzzle Palace" *Houghton Mifflin.,1982*

ii Surveillance Capitalism is a term first used by Professor Shoshana Zuboff, of The Harvard Business School, describing a new formula of catpitalism that monetizes the consumer data if collects through surveillance

iii See *The Atlantic, Apr22, 2016 "How License Plate Readers Have Hleped Police and Lenders Target the Poor"* by Kaveh Waddellm: But police don't have to do all the work themselves. A company called Vigilant Solutions claimed in a 2015 press release to maintain "the largest commercially gathered LPR dataset available to U.S. law enforcement."

iv See *The Intercept, Oct. 17, 2016 "How Israel Became a Hub for Surveillance Technology"* by Alex Kane

v See New York Times, May1, 2017 "Sent to Prison by a Software Program's Secret Algorithms" by Adam liptak, where defendant's senternce was calculated by a software program with a secret algorithm not made available to the defense

vi "Schrodinger's cat" is an expression drawn from the work of Erwin Schrodinger to imagine the effects in the physical world of the quantum theory that theorized that atoms or photons exist in multiple states that correspond with different possible outcomes.

vii End-to-end encryption ensures that only the sender and the designated recipients can know the content of a communication.

viii "Roomba maker may share maps of users' homes with Google, Amazon or Apple" by Alex Hern, The Guardian , 7/25/2017

ix See Ars Technica,2/5/201, by Ron Amadeo: *"iRobot Sells off Military Unit, will Stick to Friendlier Consumer Robots"*

x See *Disrupt SF* July 28, 2017 by B. Heater, "iRobot says the company never planned to sell Roomba home mapping data

xi Name and address for demonstration only, there is no John and Leslie Herald on Pine Shore

xii United States v. Miller 425 U.S. 435 (1976) The subpoenaed materials were business records of the banks, not respondent's private papers

xiii "How to Keep a Roomba Vacuum Cleaner From Collecting Data About Your Home" Consumer Reports 7/25/2017

xiv *United States v. Jones*, 132 S.Ct. 945 (2012)

xv Surveillance technologies are in place for tapping entire states of even countries, because the United States is reported to have done it. See *The Intercept, May 19, 2014, by Ryan Devereau and Gleen Grenwald "Data Pirates of the Carribean"*

xvi Crowdsourcing is defined by Merriam Webster as the practice of obtaining needed services, ideas, or content by soliciting contributions from a large group of people and especially from the online community rather than from traditional employees or suppliers

xvii According to the Merriam Webster dictionary, a subordinate routine is a sequence of computer instructions for performing a specified task that can be used repeatedly.

xviii The Verge, Jun 29, 2017, by James Vincent

xix A telepresence machine is a robotic remotely control device through which a human operator can experience the environment at the location of the robotic device

xx It might be a feature worth developing, if O-R3 could actually vacuum the streets as well.

xxi The definition of a "Turing Test" is a test of a computer's ability to think, requiring that the covert substitution of the computer for one of the participants in a keyboard and screen dialogue should be undetectable by the remaining human participant". (quote from Dictionary.com)

xxii See Stanford University Study "Artificial Intelligence and Life in 2030, One Hundred Year Study on Artificial Intelligence and Life 2030" September 2016