The Roomba Wi-Fi connected vacuuming robot is ready to clean on demand from anywhere, anytime. Customers can use a mobile device to schedule the robot to clean up to seven times a week.

© coffeekai | iStock

Some Things About the Internet of Things

Just as the public begins to understand that the compromise of privacy is the currency of today's web commerce, along comes another category of consumer devices that extends the consumer surveillance business model from our keyboards into our living rooms. Smart appliances and home assistants are now numerous among us, described in advertising as subservient and amiable little partners to help families cope with the needs of everyday life. This new category of domestic surveillance devices is known as "the Internet of Things." This second front in the commercialization of consumer information as a marketable commodity presents a fresh challenge to digital privacy and the Fourth Amendment.

The Internet of Things has just 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 doing the bidding of its manufacturer. The "Internet" is the digital link by which the "Thing" communicates with a corporate computer server over the customer's Wi-Fi to relay all that it is gathering about the consumer into a much larger digital storehouse that combines each household's "Thing data" with all other households' "Thing data." The aggregate of all this data gathered from within the walls of people's homes becomes corporate consumer marketing intelligence obtained through a dubiously legal, pseudo-consensual collection of domestic surveillance. These private sector surveillance technologies lead into uncharted waters in which novel opportunities for law enforcement overreach are barely submerged.

Ankle Deep in Domestic Surveillance

A recent article in *The Guardian*[1] reported that iRobot, a consumer robotics company, may begin selling the floor plans of customers' homes derived from the movement data of the company's Roomba robotic vacuum cleaner. The company's CEO advised the reporter that some Roomba models generate a digital map of the floor plan of its customers' homes. Such a detailed mapping capability has real commercial value because iRobot's data buyers would be eager to know that a Roomba consumer has a dinner table that seats eight, but owns only four chairs. The undesirable consequence of a robot vacuum repeatedly moving through your home is that while it is collecting dirt, it is also collecting dirt on you.

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 measurement data and the customer's floor plan to iRobot's corporate servers. To do so, it uses laser sensors, short-range infrared, and a camera with a cockroach's view of the 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. mili-

BY SAM GUIBERSON

tary, where iRobot cut its corporate baby teeth making battlefield robots.[2]

It took only a few days of viral news coverage of this creative marketing idea from iRobot for public and tech media outcry to produce a correction.[3] The same executive issued a statement claiming that the company was misunderstood and will never sell the Roomba location mapping to third parties such as Apple, Google or Amazon,[4] but will only give the data to the companies with the consent of the customer. No sales, however, does not mean no law enforcement access, if floor mapping surveillance data is just another business record.

Police are domestic data consumers too. After a map of a living room is described as a business record, a Roomba robot vacuum cleaner becomes quite the snitch. Many of iRobot's 20 million[5] Roomba floor cleaners are gathering and updating data about every interior detail of each of their owner's homes, how it is furnished, the distance from the sofa to the hallway, and the shape and location of all objects located in the interior floor space. Any gunstocks of firearms leaning against a wall? A stack of cash under the bed? Where does the big dog like to nap? The answers are all Roomba business records for law enforcement, and all good Intel for when a no-knock entry is the order of the day. Police could obtain access to this stream of data in real time to be sure that the suspicious backpack under the dining room table that Roomba keeps running into does not move. "The Internet of Things" is more aptly named "the Internet of Things that Search Homes."

But if "my home is my castle," how can iRobot legally search my home? If this robotic mapping device had "iPolice" inscribed on top of it instead of iRobot, it would require a search warrant. A device that maps the layout and contents of a home is conducting a search. If the third-party doctrine holds sway, the data collected by Roomba is a product of the business relationship between the customer and a third-party service provider. When promiscuous surveillance of the customer becomes the default relationship with consumer technologies, it is time for a re-examination of the standard assumptions at the root of the third-party doctrine.

Reconsidering Terms of Consent

"Internet of Things" surveillance, and other similar personal data collection schemes in the "Internet of Websites," may allow Fourth Amendment advocates unexpected openings to set new limits on the third-party doctrine's applicability for the data drawn from websites and digital home appliance platforms. A business enterprise that profits on the surveillance byproducts of its interaction with its customers presents a historically unorthodox way for a third party to conduct itself. It is time to differentiate the basic premise of the third-party doctrine from that of this new corporate surveillance business model.

Every law student knows that the third-party doctrine was born in a pile of Mitch Miller's records at his local bank. In *United States v. Miller*, the Supreme Court's judgment was that Mr. Miller's sacrifice of any Fourth Amendment protections for his personal financial records was by his own choice.[6] Choosing to "bank" required a surrender of the customer's private financial information because the bank's use and control of those records was essential to the performance of banking services. Providing banking services to a customer depended, for the benefit of both parties, upon the creation and preservation of records about funds on account, funds dispensed, and funds credited. The business records in question existed for the sole purpose of accomplishing the business objectives that each party understood to be the entire scope of the services to be undertaken by the bank on behalf of a customer.

From the factual premise for the *Miller* decision, neither Mr. Miller, his bank, nor the Supreme Court could imagine a future in which a service or a product was designed to profit, not only from the services a customer desired, but also from the third party's exploitation of the information provided by the customer, about which the customer would know nothing and from which the customer could expect nothing. While Mr. Miller lived in an era when bank customers expected banks to profit from customers' 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 third-party doctrine exempts the bank customer's confidential data from Fourth Amendment protections because consent is implied by the customer's paying a bank to perform the regular services of a banking business, how could that consent extend to a distinct and undisclosed business of profiting off the collection, manipulation, and sale of otherwise Fourth 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 when a customer surrendered exclusive control over personal information to a third party, the customer knew what business the third party was in.

When a customer purchases a Roomba robot to vacuum her carpet, money is paid for a computerized, self-navigating vacuum cleaner, not for the remote hoarding of a data stream intimately mapping the interior of her apartment. In the software industry, consent is gained 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 the user. When agreeing to Roomba's EULA, the customer is conditioned by her experience with other retail purchases to believe that she is buying a robot vacuum cleaner that sucks up carpet dust, not one that draws a map of her house and the fit of her possessions within it while performing its vacuuming duties. Since software and hardware technology companies have started playing this kind of Two-Card Monte with their customers, we are likely on the verge of asking courts to review technology companies' EULAs as closely as case law.

The Roomba's EULA reads in part:

> *3. Automatic Software Updates.*
>
> *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.*

Here is the relevant excerpt from iRobot's Privacy Policy:

> *Information We Collect From Registered Devices*
>
> *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.

Does the skillfully lawyer-crafted ambiguity of the term "location mapping," added after a serial listing of technical 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 also mapping your entire house? Does such a faux disclosure of actual intentions meet the standards of consent in a relationship with a third-party business, such that it defeats the customers' right to privacy in their homes? The fact that these reporting functions can be turned off by the technically adept consumer demonstrates that they are not at all essential to vacuum functionality.[7]

The foundation of the third-party exception rests upon the customer's surrender of his privacy in a business transaction with a third party only insofar as that surrender is necessitated by the scope of services being rendered. No bank can sneak into a person's bedroom and search for a bag of cash in the closet, and then provide the location to police authorities upon request because it is in the business of handling that person's bank accounts. The legitimacy of the third-party records exception is predicated on the premise that all personal information provided to, or generated by, a third party is an essential artifact created in the ordinary course of the business service to which the customer fully understands and consents. The factual premise for the ruling in *Miller* was that Mr. Miller knew what business his bank was in.

Is floor mapping surveillance data just another business record?

How do we craft an exception to the third-party records exception, disallowing warrantless police access to all personal domestic data collection not obtained solely to allow a product or service to function? Such an exception would do little to curtail the commercialization of customers' privacy, if consumers choose to be generous with their consent, but it would do much to prevent the exploitation of such consent by law enforcement. If defense lawyers do not aggressively challenge corporate collection and law enforcement access to the fruits of the poisonous nosey 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.

Third-Party Mining of Customer Voices

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. The entire business model of web commerce is based upon the collection of consumers' behaviors made in the course of enjoying the appliance, product, or web platform provided them. This collection of consumer decisions transforms raw personal data sets into a business asset that calculates individual and collective customer tendencies to decide in favor of any purchase or opinion to which the customer is predisposed or has been conditioned.

The expansion of this technique for website-based surveillance of keyboard input to surveillance of customer voice input is well underway. Personal digital assistants from Google, Amazon, or Apple start vocally interacting with us as soon as they enter the living rooms of families willing to converse with an unassuming little device that is but a happy face painted on a corporate computer server farm.

The home assistant "Thing," when activated by a word it hears while constantly listening to the ambient sounds and conversations in the home,[8] immediately engages with its remote server for its artificial intelligence software to translate recorded human communications into something computers can work with. After the remote server has solved the math problem of what the human wants, it directs commands back to the box sitting on your end table to comply with the vocal directive to turn on the smart dishwasher, buy a ticket to a movie, or perhaps explain how to patch sheetrock.

Each of these devices is a profitable token deployed among consumers to act as a field research lab for proprietary natural language processing and artificial intelligence engineering. While the digital assistant is getting a pizza delivered, its manufacturer is likely researching how Echo best communicates with people in their own languages, as well as how Echo itself can communicate to other humans as well as people do. The commercial value is not merely in the refinements Amazon can make to its voice recognition and speech simulation software, but also in the fact that the more such devices communicate with humans, the better they learn how to use languages to reason with them. Imagine Kubrick's HAL[9] on your nightstand, with an equally nefarious hidden agenda.

Alexa, Call Frankenstein

How could using such a convenient little digital appliance offend constitutional interests? It is a relatively low bar for law enforcement to obtain warrant access to digital home assistant devices or voice-activated remote controls in order to alter the active listening mode initiation prompt. The prompt waits for a word like "Siri" to initiate an "always on" voice activation mode, similar to handheld voice activated recorders. Law enforcement using Echo or Siri like a Title III[10] surveillance bug is no alarming paradigm shift in surveillance capabilities. Law enforcement agencies have long used court-authorized eavesdropping and wiretapping to passively listen to domestic conversations, but police have never employed technology that can actually *make* conversation with the targets of a criminal investigation. This upgrade in surveillance potential stems not from a surreptitious recording capability, but from the capacity to guide verbal interactions with the suspect being surveilled. When a digital device can make conversation with its owners while under the control of law enforcement, the covert intrusion is more like a long-term undercover operation taking place in your living room than it is a wiretap.

In the computer industry, companies aspire to create an interlocking product line that spans the consumer's range of desires to ensure that no matter what product is chosen, it is one made by the same company. This is

known as creating a "walled garden" of a company's own consumer goods from which the customer chooses, rather than from all possible choices in the open market. The interactive digital home assistant, having weaponized convenience, can offer purchasing options that are to its manufacturer's advantage, rather than the customer's. By simply substituting the words "law enforcement" in place of "manufacturer," the device's goal of placing the customer in a walled garden can be reimagined as a place with higher walls and fewer gardens.

Can one conspire with a digital assistant acting out a police-inspired subterfuge? If a customer's recorded verbal search requests trend toward weapons, extremist groups or how to make things blow up, do such third-party business "voice documents" provide the requisite suspicion and evidence of predisposition to use the digital home assistant as a "cooperating individual"? Just as police handlers might advise a human CI to verbally encourage a purchase of documents, goods or travel that would constitute an act in furtherance, can the police program a digital home assistant to aid the suspect in locating a "gunsmith" undercover agent who the suspect's Echo tells him will fabricate a silencer for him? What about the coming day when the digital assistant's voice simulation is so sophisticated that the target thinks the "gunsmith" to whom his Echo placed a call is a real human co-conspirator, instead of his own Echo pretending to be one, under the remote control of police?

Long before the future day when voice-enabled devices become artificial police undercover impersonators, voice data recorded by "Things" poses a present danger if it is easily accessible to police as a "business record." Unlike Roomba, the functionality that was promised to the digital assistant customer is dependent upon the feedback loop of data being exchanged with an Amazon server off premises, hiding in its favorite cloud. 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. As with the Roomba, the confrontation with the Fourth Amendment does not come within the course of performing the service provided, but with the manufacturer's preservation and ultra-analysis of recorded voice data to fulfill a completely different, undisclosed corporate ambition.

Are customers adequately informed of, or can they even imagine, the use to which their seemingly private communications with an electronic gadget will be put in corporate research and development? Are they consenting to interact with such devices with concrete knowledge of how the users' voice records will be commercially exploited far into the future? When clicking agreement on that Google, Apple, Amazon or Microsoft EULA, is the customer made fully aware of the manufacturer's objectives for the conversational voice exchanges the customer provides? Could she possibly know the intimate scope and complexity of her own psychological analysis that artificial intelligence resources can now perform? The applicability of the third-party doctrine to this segment of the technology market stands or falls on whether the customer consents to chatting with a device that suggests bargain dress shops while also stalking her.

To demonstrate the degree of disclosure common to the End User Licensing Agreements in this market sector, these are the data retention disclosures in the terms of service for Amazon's Echo to which consumers must agree:

> 1.1 General. *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 and select Alexa Enabled Products.* [11]

The licensing agreement does not disclose the duration of storage or in what form, or any specificity as to what "services" the harvest of human voice communication will be applied to improve, either now or in the future. Do those "services" include mining the conversation's content for advertising purposes, marketing overtures concerning the subject matters referenced, psychological and physical profiling,[12] or the semantic patterns of human request and computed response? Does a naive, blanket acceptance of an ambiguous time period[13] of voice data retention and its obscure corporate exploitation establish an informed and continuing consent?

How can customers even give "informed" consent to uses of the customers' voice data about which they are not informed? A default to generalities in a licensing agreement should not open the data logs of customers' intimate spoken requests to law enforcement access on demand because they are business records, when the "business" is an undisclosed R&D project of the corporate third party that provides no product or service to the customer and which may not even currently exist.

The corporate digital archives that store either a literal or synthesized compendium of all conversational exchanges with home assistant devices form a stockpile of raw material, the data capital needed to conduct a world-changing experiment with profound surveillance potential. Having obtained a customer's consent to their terms of service, and those of millions of others the world over, the most ambitious prospectors in the voice data mining industry want much more than to build software that can understand the customer's words. The trend of their innovation suggests that the industry hopes to go beyond perfecting how computers listen to and comply with the requests of humans to perfecting how to make people listen to and comply with computers. When robots can verbally instruct humans, they can manage workers and police the streets. The next surveillance business model will extend the two dimensional realms of keyboard and voice input to three dimensional surveillance monitoring of entire communities.

iPolice: Public Life as Private Data

Policing is the ultimate surveillance platform for "the Internet of Things." In public space, the private surveillance industry can skip consumer consent and exercise a police function by gaining only municipalities' consent to surveil the public. Direct observation of the public streets would allow a combination of digital data from websites, smartphones, digital assistants and household appliances with commercially valuable data gathered from citizens'

public conversations, facial appearance, dress, gait,[14] and pedestrian routines. The private surveillance businesses would be gathering consumer information privately and publicly, in a full circle of data collection, all the while being paid for the data collected and paid for collecting the data.

The police services rendered — such as tracking suspicious persons, identifying fugitives, and reporting offenses in progress to human counterparts — would be viewed as mere overhead for a consumer surveillance enterprise, freed of its digital boundaries to track, record, and collect the life of a city. Or, just as Internet and computer companies provide free access to services and software without charge, those same companies could offer municipalities free policing in exchange for retaining and monetizing "citizen-data," just as they have consumer data. The merger and exploitation of both private corporate data collection and government data collection would be essential to perform the police function.

Today's robot cop wannabes already have the mobility, verbal communication skills, both visual and audial surveillance capabilities, as well as technologies of physical identification and artificial intelligence.[15] All robotic policing needs is a street full of citizens to practice on. Today, that street is in Dubai.

The headline of an article on the website *The Verge*[16] says that police in Dubai have a self-driving robo-car that can "scan for undesirables." This article describes a mobile surveillance unit known as the O-R3, with a 360-degree camera. "We seek to augment operations with the help of technology such as robots," Major General Abdullah Khalifa Al Marri of the Dubai Police Force is quoted as saying. "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 robot cannot go. The Dubai Police Department wants 25 percent of its police force to be robots by 2030.

In the configuration described in the article, the O-R3 is little more than a set of wheeled eyeballs walking the beat, a sort of Roomba with a badge, much dumber than an Echo. The hint of what is to come is in the article's reference to "scanning for undesirables."

Similar to Roomba and devices like Echo, the next generation of the O-R3 will use spatial and facial recognition technology that requires a sustained wireless link to a computer server running 24/7 somewhere in the cop cloud. Like the Echo, the O-R3 will become a mobile extension of a much more sophisticated, complex hierarchy of software and technology than meets the eye. OR-3, in some future iteration, will accomplish all its street-level surveillance using the full range of cloud-stored commercial and law enforcement profiling data that the technology industry and law enforcement agencies have aggregated over decades of consumer and citizen surveillance. It will behave like an Echo, but asking only itself for the answers to all of its own questions about each individual.

How much about an individual is public in a public space will steadily increase as new surveillance technologies become integrated with instant access to the most intimate captured data from one's past. Tomorrow's police surveillance platform will roll around the streets like a riding lawn mower, making decisions as a human officer's surrogate, drawing from a data field larger than that of the police departments of all law enforcement officers who ever walked its beat — and it will also know where you bought your watch.

The coupling of police records and private industry data greatly enriches this new surveillance collaboration of government and private industry. As the next generation of private police robots steer through the streets, they will tirelessly add to that ocean-deep digital archive of personal surveillance data with which corporate and government interests can get to know the citizenry well enough to either profit off them or put them in their places. Just as it is with the Internet, there will be no anonymity in a crowd, nor privacy when alone in public.

After reaching this point of no return, no private police surveillance platform will have to ask a consumer end user for his consent, as have previous consumer surveillance devices. The "end user" of the surveillance technologies in the streets will not be an individual customer: the third-party doctrine will become irrelevant when the only consenting customer is the police. The challenge is to decide whether private industry's interest in surveilling the public is in the public interest, and whether the public's social contract with the government is to be defined by an End User Licensing Agreement or the Constitution.

Notes

1. Alex Hern, *Roomba Maker May Share Maps of Users' Homes With Google, Amazon or Apple,* THE GUARDIAN, July 25, 2017, and for more background, see Maggie Astor, *Your Roomba May be Mapping Your Home Collecting Data That Could Be Shared,* N.Y. TIMES, July 25, 2017.

2. Ron Amadeo, *iRobot Sells off Military Unit, Will Stick to Friendlier Consumer Robots,* ARS TECHNICA, Feb. 5, 2017.

3. See Reuters article correction by Reuters Staff, *Roomba Vacuum Cleaner Maker iRobot Betting Big on the 'Smart' Home,* REUTERS, July 24, 2017.

4. See B. Heater, *iRobot Says the Company Never Planned to Sell Roomba Home Mapping Data,* DISRUPT SF, July 28, 2017.

5. The iRobot "has sold more than 20 million robots worldwide." See www.irobot.com/About-iRobot/Company-Information/History.

6. *United States v. Miller,* 425 U.S. 435 (1976). "All of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business." 425 U.S. at 442 (Powell, J).

7. Allen St. John, *How to Keep a Roomba Vacuum Cleaner From Collecting Data About Your Home,* CONSUMER REPORTS, July 31, 2017.

8. See Jay Stanley, *The Privacy Threat From Always-On Microphones Like the Amazon Echo,* www.aclu.org/blog/privacy-technology/privacy-threat-always-microphones-amazon-echo, Jan. 13, 2017 (for a discussion of the broader issue of always-on microphones and the 2017 Arkansas murder case in which a warrant for Echo recordings was resisted by Amazon before the issue was mooted by the Echo owner's consent and the case dismissed).

9. In the 1968 science fiction classic, *2001: A Space Odyssey,* directed by Stanley Kubrick, an intelligent, articulate computer named HAL operates the interplanetary spaceship and converses amiably with the crew, while plotting their elimination.

10. Title III of The Omnibus Crime Control and Safe Streets Act of 1968 (Wiretap Act) 18 U.S.C. §§ 2510-22, as amended by the Electronic Communications Privacy Act (ECPA), controls court authorization for the monitoring of oral communications.

11. Read the entire Amazon EULA at https://www.amazon.com/gp/help/customer/display.html?nodeId=201809740.

12. Jamie Condliffe, *Amazon's Echo Look Rates Your Outfits and Slurps Up Revealing Data,* www.technologyreview.com/s/604284/amazons-echo-look-rates-your-

outfits-and-slurps-up-revealing-data. *See also* James Vincent, *Amazon's Echo Look Is a Minefield of AI and Privacy Concerns*, THE VERGE, April 17, 2017.

13. The term of retention for voice samples and the term of their use in corporate are not necessarily the same. "While Apple logs and stores Siri verbal queries, they're tied to a random string of numbers for each user instead of an Apple ID or email address. Apple deletes the association between those queries and those numerical codes after six months. Your Amazon and Google histories, on the other hand, stay there until you decide to delete them." Dan Moynihan, *Alexa and Google Home Record What You Say. But What Happens to That Data?"* WIRED MAGAZINE, Dec. 5, 2016. Read this article to learn how to delete what voice records you can.

14. "The Chinese facial recognition company Cloud Walk Technology is trying to actually predict if an individual will commit a crime before it happens. The company plans to use facial recognition and gait analysis technology help the government use advanced AI to find and track individuals." Daniel Faggella, *AI for Crime Prevention and Detection — 5 Current Applications*, www.techemergence.com, Nov. 13, 2017.

15. Major players in the auto industry are currently seeking patents for autonomous policing vehicles. See Peter Holley, *Ford Wants to Patent a Driverless Police Car That Ambushes Lawbreakers Using Artificial Intelligence*, WASH. POST, Jan. 31, 2018.

16. James Vincent, *Police in Dubai Have Recruited a Self-Driving Robo-Car That Can 'Scan for Undesirables,'* THE VERGE, www.theverge.com/2017/6/29/15893802/dubai-police-robot-drone-car, 06/29/17. ■

About the Author

Sam Guiberson assists fellow NACDL members in cases with undercover recordings, voice and data communications surveillance, digital search and seizure, and "Things" stuff from discovery through trial.

Sam Guiberson
Guiberson Law Offices, PLC
713-520-7200
WEBSITE www.guiberson.com
EMAIL sam@guiberson.com

NACDL® STAFF DIRECTORY

MEMBERSHIP HOTLINE 202-872-4001

Senior Resource Counsel	Vanessa Antoun	202-465-7663	vantoun@nacdl.org
Education Manager	Akvile Athanason	202-465-7630	aathanason@nacdl.org
Administrative Assistant	Tatum A. Brooks	202-465-7657	tbrooks@nacdl.org
Education Assistant	Shuli Carroll	202-465-7643	scarroll@nacdl.org
Deputy Executive Director	Tom Chambers	202-465-7625	tchambers@nacdl.org
Editor, The Champion®	Quintin Chatman	202-465-7633	qchatman@nacdl.org
Membership Director	Michael Connor	202-465-7654	mconnor@nacdl.org
Resource Counsel	Jessica DaSilva	202-465-7646	jdasilva@nacdl.org
Director of Public Affairs & Communications	Ivan Dominguez	202-465-7662	idominguez@nacdl.org
Senior Advisor for Special Projects	Angelyn C. Frazer-Giles	202-465-7642	afrazer-giles@nacdl.org
Public Affairs & Communications Assistant	Alexandra Funk	202-465-7647	afunk@nacdl.org
Junior Graphic Designer	Julian Giles	202-465-7655	jgiles@nacdl.org
Director of Public Defense Reform and Training	Bonnie Hoffman	202-465-7649	bhoffman@nacdl.org
Director of Events	Tamara Kalacevic	202-465-7641	tkalacevic@nacdl.org
White Collar Crime Policy Counsel	Caleb Kruckenberg	202-465-7652	ckruckenberg@nacdl.org
Associate Executive Director for Programs, Business Services, and Technology	Gerald Lippert	202-465-7636	glippert@nacdl.org
Senior Privacy and National Security Counsel	Jumana Musa	202-465-7658	jmusa@nacdl.org
Public Affairs & Communications Assistant	Ian Nawalinski	202-465-7624	inawalinski@nacdl.org
Associate Executive Director for Policy	Kyle O'Dowd	202-465-7626	kodowd@nacdl.org
Senior Manager for Advocacy	Monica L. Reid	202-465-7660	mreid@nacdl.org
Executive Director	Norman L. Reimer	202-465-7623	nreimer@nacdl.org
Graphics Assistant	Saira Rivera	202-465-7635	srivera@nacdl.org
Member Services Assistant	Nelle Sandridge	202-465-7639	nsandridge@nacdl.org
Production Design Assistant	Zach Schermerhorn	202-465-7635	zschermerhorn@nacdl.org
National Affairs Associate	Lisa Ama Schrade	202-465-7638	lschrade@nacdl.org
Senior Membership and Operations Associate	Viviana Sejas	202-465-7632	vsejas@nacdl.org
Information Services Manager	Doug Shaner	202-465-7648	dshaner@nacdl.org
Public Defense Reform and Training Counsel	Renee Spence	202-465-7651	rspence@nacdl.org
Chief Financial Officer	Richard K. Stanley	202-465-7644	rstanley@nacdl.org
Associate Executive Director for Strategic Marketing	Jessica Stepan	202-465-7629	jstepan@nacdl.org
Manager — Multimedia Production & Sales	Koichi Take	202-465-7661	ktake@nacdl.org
Fourth Amendment Center Education and Research Associate	Kian Vesteinsson	202-465-7659	kvesteinsson@nacdl.org
Foundation Manager and Executive Assistant	Daniel Weir	202-465-7640	dweir@nacdl.org
Art Director	Catherine Zlomek	202-465-7634	czlomek@nacdl.org

03202018