BAIT, MASK, AND RUSE: TECHNOLOGY AND POLICE DECEPTION

Elizabeth E. Joh[*]

Deception and enticement have long been tools of the police, but new technologies have enabled investigative deceit to become more powerful and pervasive. Most of the attention given to today's advances in police technology tends to focus either on online government surveillance[1] or on the use of algorithms for predictive policing or threat assessment.[2] No less important but less well known, however, are the enhanced capacities of the police to bait, lure, and dissemble in order to investigate crime. What are these new deceptive capabilities, and what is their importance?

Misrepresentation by the police can take many forms. The police may deceive by concealing their identity, their purpose, or both. Police conceal their purpose when they try to convince a suspect to open his door by asking for help in locating a fictitious person. They conceal both their identity and purpose when they pretend to be mobsters or potential robbery victims. Covert policing of this second type has greatly expanded over time; a recent *New York Times* investigation estimated that there are thousands of undercover agents at the federal level alone.[3] Consider the new world of baits, masks, and ruses.

Baits: While offering attractive targets to entice potential thieves is not new, the baiting capabilities of the police are. Small GPS trackers can be embedded into everyday items, and their low cost means that police departments can use them to investigate many different crimes. For example, the NYPD has planted "bait bottles" with GPS trackers in drugstores to catch OxyContin thieves.[4] Albuquerque police have

---

[*] Professor of Law, University of California, Davis, School of Law (eejoh@ucdavis.edu). Thanks to Andrew Ferguson, Thomas Joo, and Charles Reichmann for comments.

[1] *See, e.g.*, United States v. Garcia, 474 F.3d 994, 998 (7th Cir. 2007) ("Technological progress poses a threat to privacy by enabling an extent of surveillance that in earlier times would have been prohibitively expensive," and thus "giv[es] the police access to surveillance techniques that are ever cheaper and ever more effective.").

[2] *See, e.g.*, Erica Goode, *Sending the Police Before There's a Crime*, N.Y. TIMES (Aug. 15, 2011), http://www.nytimes.com/2011/08/16/us/16police.html.

[3] Eric Lichtblau & William M. Arkin, *More Federal Agencies Are Using Undercover Operations*, N.Y. TIMES (Nov. 15, 2014), http://www.nytimes.com/2014/11/16/us/more-federal-agencies-are-using-undercover-operations.html.

[4] Joseph Goldstein, *Police to Use Fake Pill Bottles to Track Drugstore Thieves*, N.Y. TIMES (Jan. 15, 2013), http://www.nytimes.com/2013/01/16/nyregion/ny-police-to-track-drugstore-robbers-via-decoy-bottles.html; Chris Matyszczyk, *NYPD Uses GPS-Enabled Pill Bottle to Catch Alleged Drugstore Robber*, CNET (May 18, 2014, 11:30 AM), http://www.cnet.com/news/nypd-uses-gps-enabled-pill-bottle-to-catch-drugstore-robber [http://perma.cc/6TBG-MJGZ].

created a "bait house" replete with GPS-embedded items.[5] The San Francisco police have successfully used GPS-tracked bait bikes (and Twitter) to combat bicycle theft.[6] Many local police departments have used bait cars with GPS trackers to investigate auto theft.[7]

These GPS-embedded baits can then be tracked remotely, away from the scene. If the emerging "Internet of things" provides us with remote access to our thermostats, garage door openers, and household locks through small embedded sensors and the Internet,[8] we might think of GPS baits as a parallel *criminal Internet of things* that connects police to contraband decoys. Cheap and small GPS trackers have made it feasible to bait all sorts of items to see if they end up in criminal hands.

Masks: The masked identities of undercover police agents, especially those who infiltrate organized crime, are staples of film and fiction. Being accepted into a gang or the Mafia by aping its members' dress, speech, and mannerisms requires risk taking and skill. While not every officer can be Joe Pistone (a.k.a. "Donnie Brasco") in real life,[9] identity simulation has become easier online. If private individuals can hide their gender, age, or race online, so too can the police. Thus police officers have pretended to be seniors, minors, or criminals who might ask to "friend" a suspect on Facebook[10] or Instagram.[11]

In two recent examples, law enforcement agencies even engaged in a kind of identity theft in order to investigate crime. In one case, a

---

[5] *"Bait" House Snags Would-Be Thief*, KOAT-TV (June 22, 2013, 10:04 AM), http://www.koat.com/news/new-mexico/albuquerque/bait-house-snags-wouldbe-thief/20674646 [http://perma.cc/2LWR-KU46].

[6] Matt Richtel, *Police Use High-Tech Lures to Reel in Bike Thieves*, N.Y. TIMES (May 27, 2014), http://www.nytimes.com/2014/05/28/us/police-use-high-tech-lures-to-reel-in-bike-thieves.html.

[7] *E.g.*, Tristan Hallman, *Dallas Police to Ask for More Bait Cars*, DAL. MORNING NEWS (Apr. 28, 2014, 10:57 PM), http://www.dallasnews.com/news/metro/20140428-dallas-police-to-ask-for-more-bait-cars.ece [http://perma.cc/S292-K4T3]; KOAT-TV, *supra* note 5.

[8] Jacob Morgan, *A Simple Explanation of "The Internet of Things,"* FORBES (May 13, 2014, 12:05 AM), http://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand [https://perma.cc/CX9Z-MWQN?type=source].

[9] *See generally* JOSEPH D. PISTONE, DONNIE BRASCO: MY UNDERCOVER LIFE IN THE MAFIA (1988).

[10] *See* Richard Lardner, *Your New Facebook "Friend" May Be the FBI*, NBC NEWS (Mar. 16, 2010, 10:54 AM), http://www.nbcnews.com/id/35890739/ns/technology_and_science-security/t/your-new-facebook-friend-may-be-fbi [http://perma.cc/X77V-TU65].

[11] *See* United States v. Gatson, Criminal No. 13-705, 2014 WL 7182275, at *22 (D.N.J. Dec. 15, 2014); Cyrus Farivar, *Judge: It's OK for Cops to Create Fake Instagram Accounts*, ARS TECHNICA (Dec. 20, 2014, 11:00 AM), http://arstechnica.com/tech-policy/2014/12/judge-its-ok-for-cops-to-create-a-fake-instagram-account-friend-you [http://perma.cc/P4CU-FL2D]; *see also* GLOBAL JUSTICE INFO. SHARING INITIATIVE, DEVELOPING A POLICY ON THE USE OF SOCIAL MEDIA IN INTELLIGENCE AND INVESTIGATIVE ACTIVITIES 14 (2013), http://www.iacpsocialmedia.org/Portals/1/documents/SMInvestigativeGuidance.pdf [http://perma.cc/5CNE-8J2B] (recommending adoption of policies for covert online investigations).

DEA agent established a fake Facebook account by impersonating a woman's real identity online, without her consent or knowledge.[12] The DEA agent hoped to use the account, containing photos taken from the woman's cellphone upon her arrest, to find others related to a drug investigation.[13] In another case, the FBI, purporting to be the Associated Press, in 2007 sent a MySpace message to a person suspected of sending bomb threats to a Washington state high school.[14] Within the message was a link containing malware which, when clicked, identified the location of the teenage suspect, who was subsequently arrested and then pled guilty.[15]

Ruses: Police have long used ruses in order to trick and lure suspects into providing evidence or admitting guilt. Now that it is possible to extract DNA from very small samples accurately and cheaply, police have tricked suspects into giving up DNA samples contained in saliva left behind on ordinary objects.[16] These cases typically arise when the police suspect the person of a crime but lack the ability to obtain a warrant to compel a DNA sample. Instead, the police collect the person's DNA through deception and misrepresentation. Police have obtained DNA samples by convincing a suspect to lick a stamp,[17]

---

[12] Jacob Gershman, *U.S. to Pay Woman $134,000 for Impersonating Her on Facebook*, WALL ST. J.L. BLOG (Jan. 20, 2015, 8:02 PM), http://blogs.wsj.com/law/2015/01/20/u-s-to-pay-woman-134000-for-impersonating-her-on-facebook. The settlement did not prohibit future use of this impersonation technique. *See* Stipulation for Voluntary Dismissal, Compromise Settlement, and Release of Claims, Arquiett v. United States, No. 13-CV-0752 (N.D.N.Y. Jan. 20, 2015), http://online.wsj.com/public/resources/documents/2015_0120_Arquiettsettlement.pdf.

[13] Gershman, *supra* note 12.

[14] Ellen Nakashima & Paul Farhi, *FBI Agent Impersonated AP Reporter in Hunt for Teenage Suspect, Director Confirms*, WASH. POST (Nov. 7, 2014), http://www.washingtonpost.com/lifestyle/style/fbi-agents-impersonated-ap-reporter-in-hunt-for-teenage-suspect-director-confirms/2014/11/07/22455272-6696-11e4-9fdc-d43b053ecb4d_story.html [http://perma.cc/8W8C-D343]; Catherine Taibi, Seattle Times *"Outraged" over FBI's Fake News Story to Catch Bomb-Threat Suspect*, HUFFINGTON POST (Oct. 29, 2014, 2:59 PM), http://www.huffingtonpost.com/2014/10/28/fbi-seattle-times-fake-web-page-bomb-threat-suspect_n_6061082.html [http://perma.cc/M49Z-PQTZ].

[15] Taibi, *supra* note 14. While the operation was conducted in 2007, news of the tactic was not reported until October 2014, when documentation was discovered by the Electronic Frontier Foundation through a Freedom of Information Act request. *See* Lily Hay Newman, *The FBI Used Malware and a Fake* Seattle Times *Article Page to Track a Bomb Threat Suspect*, SLATE: FUTURE TENSE (Oct. 28, 2014, 3:02 PM), http://www.slate.com/blogs/future_tense/2014/10/28/the_fbi_made_a_malware_spreading_seattle_times_article_to_track_bomb_threat.html [http://perma.cc/V3S9-8TE2].

[16] *See* Albert E. Scherr, *Genetic Privacy & the Fourth Amendment: Unregulated Surreptitious DNA Harvesting*, 47 GA. L. REV. 445, 450–51 (2013).

[17] *See* State v. Athan, 158 P.3d 27 (Wash. 2007). In *Athan*, police detectives obtained Athan's DNA sample after posing as a fake law firm and sending Athan a letter asking him to join a fake class action lawsuit. Athan's DNA sample was collected from saliva located on the envelope flap. *Id.* at 31–32.

or by inviting the person for a meal or conversation and later collecting DNA from the cup or straw left behind.[18]

These examples show how technology has made deceptive policing easier and more pervasive than traditional means ever did. Police have long set out baited goods, but this required personal observation by police officers, not remote, computer-assisted monitoring at the police station. Police have also long pretended to be criminals, but this required the selection of officers both sufficiently skilled and physically similar to those in the criminal underworld to be convincing in their impersonations. Finally, while traditional police investigations have also sought to collect other identity evidence from suspects, it is now easy and cheap for the police to obtain a DNA sample containing the entirety of your genetic information through deceit.

These changes are troubling because they erode already weak doctrinal safeguards against police deception. Entrapment law permits defendants to raise a defense when the government creates criminals rather than just providing them with an opportunity to commit crime, as in the case of unusually enticing bait.[19] Yet, in practice, entrapment is a losing defense. For most courts, the conclusion that a defendant is criminally predisposed to commit the offense bars an entrapment claim even where the government's temptations may be unrealistically attractive.[20]

For defendants outwitted by false friends who turn out to be the police in disguise, Fourth Amendment claims are equally unavailing. As the Supreme Court observed in *Hoffa v. United States*,[21] people assume the risk that the confidences they share with others they believe to be criminal associates may turn out to be "misplaced."[22]

Finally, those targeted by police ruses in order to collect DNA samples have similarly weak claims on their genetic privacy. Courts have routinely permitted the police to engage in a variety of ruses to obtain evidence. Even more difficult for those who unwittingly provide DNA samples to the police, courts typically deem the information

---

[18] *See, e.g.*, Commonwealth v. Ewing, 854 N.E.2d 993, 1000–01 (Mass. App. Ct. 2006) (concluding that even if police engaged in ruse to obtain DNA by offering defendant food and cigarettes, deception was "proper," *id.* at 1001); People v. LaGuerre, 815 N.Y.S.2d 211, 213 (App. Div. 2006) (finding no due process violation when police conducted a "contrived Pepsi taste test challenge" to retrieve the defendant's DNA sample).

[19] *See, e.g.*, United States v. Mayfield, 771 F.3d 417, 434–35 (7th Cir. 2014) (en banc) ("[Improper] inducement means government solicitation of the crime *plus* some other government conduct that creates a risk that a person who would not commit the crime if left to his own devices will do so . . . .").

[20] *See, e.g.*, United States v. Díaz-Maldonado, 727 F.3d 130, 139 (1st Cir. 2013) ("[T]he entrapment defense is a difficult defense to raise and prevail on.").

[21] 385 U.S. 293 (1966).

[22] *See id.* at 302 (holding that the Fourth Amendment does not protect "a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it").

to have been "abandoned," and thus without any Fourth Amendment protection in the first place.[23]

The law regulating investigative deception may be weak because police have traditionally been limited by practical, not legal, constraints — which are disappearing as well. Consider the Supreme Court's 2012 decision in *United States v. Jones*.[24] Justice Alito's observation in his concurring opinion is especially telling: "[T]he greatest protections of privacy [until now have been] . . . practical," because "[t]raditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken."[25] The undoing of practical constraints has been no less powerful in the context of deceptive policing. Using traditional decoys requires considerable human resources and technical assistance. In traditional policing, only limited numbers of officers can pretend to be young women, minors, or members of racial minorities. Finally, gleaning genetic information from leftover biological samples in affordable and reliable ways is a product of the very recent past.

From the perspective of the police, investigative deception is becoming easy and cheap. Like closed-circuit television cameras, these deceptive means are "force multipliers" for the police. Rather than a special technique available to only a few departments, these technological means of deception can be used by many departments for many different crimes.

These new types of baits, masks, and ruses also raise troubling questions about the costs to social trust that result when the government is able to engage in unconstrained, open-ended investigations of the population. While some of these technologically enhanced means are used against suspects that are identified in advance, many of these technological stings amount to generalized "fishing": attempts to find out if anyone will be tempted by the proper enticement.[26] There are no doctrinal bars to such open-ended traps. Police are not bound by probable cause or reasonable suspicion requirements before they engage in a sting.[27]

When we know that the government engages in open-ended fishing for crime and information — both in the real world and in the virtual one — such testing can undermine social trust. Just as many people

---

[23] *See, e.g.*, State v. Williford, No. COA14-50, 2015 WL 67145, at *4–5 (N.C. Ct. App. Jan. 6, 2015) (collecting recent cases).

[24] 132 S. Ct. 945 (2012).

[25] *Id.* at 963 (Alito, J., concurring in the judgment).

[26] GARY T. MARX, UNDERCOVER: POLICE SURVEILLANCE IN AMERICA 70 (1988).

[27] *See* United States v. Jacobson, 916 F.2d 467, 469 (8th Cir. 1990) (en banc) ("[T]he constitution does not require reasonable suspicion of wrongdoing before the government can begin an undercover investigation."), *rev'd on other grounds*, 503 U.S. 540 (1992).

worry about the threat to our privacy posed by secret government surveillance of our online activities, so too should we be concerned when pervasive government deception promotes uncertainty about the true identity of people and objects around us. When news of the FBI's impersonation of the Associated Press emerged in October 2014, several news media organizations, including the Associated Press, *Washington Post*, and *New York Times*, expressed alarm at the tactic's potential to undermine trust in a free press.[28]

Similarly, if police can easily and legally trick you out of your DNA sample, then we may have good cause to feel a little helpless and paranoid. Just as it is nearly impossible to avoid leaving a digital trail behind, it is also nearly impossible to avoid leaving your genetic traces everywhere. In a small number of states it may be illegal for private individuals to collect your DNA without consent, but you're out of luck when it comes to the police.[29]

To be sure, these deceptions sometimes catch serious criminals. But deception can involve situations where the crime involved is ambiguous, or the government enticement dubious. Yet the basic legal framework behind these investigative lies — that those caught in these traps have assumed the risk — gives nearly unbridled discretion to the police. Police decisions about how, whether, and against whom such misrepresentations can be targeted do not typically receive any external review.[30]

The combination of wide discretion and sophisticated technology may lead to tactics that raise further ethical questions. If the police are not obliged to conduct immediate arrests, why not use bait for surveillance, or to obtain a DNA sample? If the police can "friend" potential sex offenders, why not members of protest groups? If the police trick a suspect out of his DNA sample, why not trick an innocent person who may have genetic ties to a potential suspect?

If the prospect of pervasive government surveillance threatens individual privacy, then the reach of today's deceptive policing should

---

[28] *See, e.g.*, Letter from Karen Kaiser, Gen. Counsel, Associated Press, to Eric Holder, Att'y Gen., Dep't of Justice (Oct. 30, 2014), https://corpcommap.files.wordpress.com/2014/10/letter_103014.pdf [https://perma.cc/STQ4-RA62] ; Editorial, *By Impersonating Reporters, the FBI Undermines Their Credibility*, WASH. POST (Nov. 10, 2014), http://www.washingtonpost.com/opinions/by-impersonating-reporters-the-fbi-undermines-their-credibility/2014/11/10/85d44baa-684d-11e4-a31c-77759fc1eacc_story.html [http://perma.cc/6EWG-HF5F]; Editorial, *Deceptions of the F.B.I.*, N.Y. TIMES (Oct. 31, 2014), http://www.nytimes.com/2014/11/01/opinion/deceptions-of-the-fbi.html.

[29] *See* Elizabeth E. Joh, *DNA Theft: Recognizing the Crime of Nonconsensual Genetic Collection and Testing*, 91 B.U. L. REV. 665, 686–89 (2011).

[30] *See, e.g.*, Elizabeth E. Joh, *Breaking the Law to Enforce It: Undercover Police Participation in Crime*, 62 STAN. L. REV. 155, 188 (2009).

also give us pause. If privacy should not be a luxury good,[31] neither should trust in our society or government. Suspicions that objects are embedded with police bait, that police stratagems might lie behind seemingly private online encounters, or even that police interactions might secretly target genetic information are not the stuff of science fiction. These high-tech police deceptions exist, and are increasingly becoming part of ordinary police practice. And that's no lie.

[31] Julia Angwin, Op-Ed., *Has Privacy Become A Luxury Good?*, N.Y. TIMES (Mar. 3, 2014), http://www.nytimes.com/2014/03/04/opinion/has-privacy-become-a-luxury-good.html.