1

2

3

of material information in a warrant application prevents the court from exercising this constitutional function. *United States v. Rettig*, 589 F.2d 418, 422-23 (9th Cir. 1979). Judicial supervision is particularly important with evolving technology, where there is a heightened risk of overly intrusive searches. *See United States v. Comprehensive Drug Testing, Inc.* (*CDT*), 621 F.3d 1162, 1176 (9th Cir. 2010) (en banc).

locations of the target and third parties in the area.[6] Depending on the device's signal strength, the broadcast radius can reach up to "several kilometers."[7]

Third, the devices can pinpoint an individual with extraordinary precision, in some cases "within an accuracy of 2 m[eters]."[8] The government has conceded that the device located Mr. Rigmaiden precisely *within* his apartment. Order, Doc. 723 at 15, 19.

Fourth, although the specific device used by the FBI in this case may have been configured not to intercept content, materials from several surveillance vendors selling IMSI catchers show that these devices are certainly capable of doing so.[9]

The government's use of the stingray violated the Fourth Amendment

[6] The devices send signals like those emitted by a carrier's own base stations. *See, e.g.,* Harris Corp. product sheet at 1 ("Active interrogation capability emulates base stations"), *available at* http://servv89pn0aj.sn.sourcedns.com/~gbpprorg/2600/Harris_StingRay.pdf. Those signals, of course, "penetrate walls" (necessarily, to provide connectivity indoors). *What You Need to Know About Your Network,* AT&T, http://www.att.com/gen/press-room?pid=14003; *see also* E.H. Walker, *Penetration of Radio Signals Into Buildings in the Cellular Radio Environment*, 62 THE BELL SYSTEMS TECHNICAL JOURNAL 2719 (1983), *available at* http://www.alcatel-lucent.com/bstj/vol62-1983/articles/bstj62-9-2719.pdf.

[7] Strobel, *supra*, note 4, at 13.

[8] *See, e.g.,* "GSM Cellular Monitoring Systems" brochure by PKI Electronic Intelligence GmbH at 12 (device can "locat[e]... a target mobile phone within an accuracy of 2 m[eters]"), *available at* http://www.docstoc.com/docs/99662489/GSM-CELLULAR-MONITORING-SYSTEMS---PKI-Electronic-#; Resp. to National Telecommunications Information Administration Notice of Inquiry (Doc. #100504212-0212-01) Requesting Information on Preventing Contraband Cell Phone Use in Prisons, submitted by Bahia 21 Corp. at 3 (June 11, 2010), *available at* http://www.ntia.doc.gov/files/ntia/comments/100504212-0212-01/attachments/BAHIA21%20resposne%20to%20NTIA%20NOI.pdf (a US surveillance vendor offering fixed IMSI catchers to be installed in prisons to detect contraband cell phones, promising 10-15m accuracy of geolocation identification) .

[9] *See, e.g.,* Harris, Wireless Products Group Price List at 8 (September 2008) (StingRay line of products includes "Intercept Software Package" for GSM phones),

> fixes the geographic position of the Target Broadband Access Card/Cellular Telephone.

Affidavit at ¶42 (emphasis added). Particularly because the Application sought Verizon's assistance, these two sentences suggest that *Verizon* would determine the lo 54.vie

the Order would be an unconstitutional "general warrant." By failing to apprise the magistrate that it intended to use a stingray, what the device is, and how it works, it prevented the judge from exercising his constitutional function of ensuring that warrants

cell phone information of suspect and third parties). Had the court been alerted to the existence of this issue, it might have developed a procedure other than wholesale data purging, such as "[s]egregation and redaction" of third-party information "by specialized personnel or an independent third party." *See CDT*, 621 F.3d at 1180 (Kozinski, C.J., concurring). It was for the magistrate, not the government, to determine how best to balance the government's need for information, third-party privacy, and the suspect's interest in future access to potentially exculpatory information.

parties as to whom it lacked probable cause. Where the government engages in a search pursuant to a general warrant, "we must regard the search as 'warrantless'…" *Groh v. Ramirez*, 540 U.S. 551, 558 (2004).[16]

Given the heightened risk of intrusive searches posed by advances in technology, "the government's duty of candor in presenting a warrant application," *CDT*, 621 F.3d at 1178 (Kozinski, C.J., concurring), requires it to explain to magistrates the technology and "the process by which the technology will be used to engage in the electronic surveillance." *In re Stingray*, 2012 WL 2120492 at *1. In light of their impact on third parties and their potential to capture content, IMSI catchers are a potent illustration of the Ninth Circuit's concern in *CDT* that absent judicial supervision, warrants authorizing electronic searches risk becoming "general warrant[s], rendering the Fourth Amendment irrelevant." 621 F.3d at 1176.[17]

The government contends that Mr. Rigmaiden lacks standing to raise this Fourth Amendment challenge because his use of an alias rendered his privacy expectation objectively unreasonable. *See Rakas v. Illinois*, 439 U.S. 128, 143 n.12 (1978) (defendant must prove subjective and objective expectation of privacy).[18] This argument is meritless.

First, even if the analysis turned solely on the aircard, the privacy interest is not simply in using an alias to engage in an ordinary commercial transaction, but in an

[16] The government's reliance on *Karo* is misplaced. *See* Gov's. Resp., Doc. 873 at 52. The Court in *Karo* stated "it will still be possible to describe the object into which the beeper is to be placed" and suggested that such information (along with probable cause and the duration of the proposed surveillance) would suffice. 468 U.S. at 718. Even with a beeper, which has far less technological capacity for intrusion than a stingray, the Court expected the government to explain the basic methodology of the proposed electronic surveillance (that the government intended to install a beeper at all, and where it sought to do so). The government here withheld from the judge the pertinent analogous information.

[17] There is a serious question whether stingray technology – because of its inevitable impact on third parties – can ever be used consistent with the Fourth Amendment. But the Court can conclude that the stingray search in this case violated the Fourth Amendment on scope or particularity grounds.

[18] The government does not dispute that Mr. Rigmaiden manifested a subjective expectation of privacy.

inherently expressive activity, accessing the internet anonymously. Mr. Rigmaiden has a legitimate expectation of privacy in his aircard because the constitutional right to anonymous internet speech is surely "one that society is prepared to recognize as reasonable." *Katz v. United States,* 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

"The internet is a unique democratizing medium unlike anything that has come before….Through the internet, speakers can bypass mainstream media to speak directly to 'an audience larger and more diverse than any the framers could have imagined.'" *Doe v. Cahill*, 884 A.2d 451, 455-56 (Del. 2005) (citation omitted). "Under our constitution, anonymous [speech] … is not a pernicious, fraudulent practice, but an honorable traditiernet speech is su

proposition that use of an alias forecloses a reasonable privacy expectation. In *United States v. Pitts*, 322 F.3d 449 (7th Cir. 2003), the court upheld a search of a package mailed to a fictitious name, but on the very different ground that the defendants had abandoned the parcel. *Id.* at 455. The majority went on to criticize the concurrence cited by the government: The refusal of the concurrence in *Pitts* – and the government here – to recognize a legitimate privacy expectation because of the alias either means that "everyone with a legitimate reason to remain anonymous should lose their expectation of privacy in the post" simply "because some people employ an alias and use the mail illegally," or that "only people using an alias for legitimate reasons may retain an expectation of privacy in their mailings while those who employ an alias for illicit purposes may not." *Id.* at 458. This Court should not embrace a theory that "turn[s] the Fourth Amendment on its head." *Id.*

Most of the government's alias cases rest on the unremarkable proposition that one cannot assert a privacy expectation in the property of another, and as a result, reject the defendant's assertion of a reasonable privacy expectation "when an individual uses an alias or fictitious name *and there is no other evidence linking the defendant to2 td[(t)-6(h)-4(at)-(k5Tw - )]*

Second, the government's focus on the aircard is misplaced. Mr. Rigmaiden has standing because he has an undisputed privacy expectation in the *place*

Dated: October 19, 2012 Respectfully submitted,

CERTIFICATE OF SERVICE

I hereby certify that on