

UNITED STATES DISTRICT COURT  
DISTRICT OF ARIZONA

United States of America,  
Plaintiff

v.

Daniel David Rigmaiden, et al.,  
Defendant.

No. CR08-814-PHX-DGC

BRIEF OF RESEARCHERS AND EXPERTS, *PRO SE*,  
AS *AMICI CURIAE* IN SUPPORT OF DEFENDANT’S MOTION FOR DISCLOSURE OF ALL  
RELEVANT AND HELPFUL EVIDENCE WITHHELD BY THE GOVERNMENT  
BASED ON A CLAIM OF PRIVILEGE

**Table of Contents**

STATEMENT OF INTEREST OF *AMICI CURIAE* ..... 1

SUMMARY OF ARGUMENT ..... 1

INTRODUCTION..... 2

IMSI CATCHERS HAVE BEEN SOLD BY COMMERCIAL SURVEILLANCE VENDORS FOR  
MORE THAN FIFTEEN YEARS ..... 3

SURVEILLANCE VENDORS PROUDLY ADVERTISE THEIR IMSI CATCHERS AND  
DESCRIBE THEIR FEATURES IN PUBLIC MARKETING MATERIALS ..... 4

A SUBSTANTIAL AMOUNT OF DETAILED TECHNICAL INFORMATION ABOUT IMSI  
CATCHERS IS ALREADY PUBLIC ..... 7

IMSI CATCHERS CAN NOW BE BUILT FOR \$1500 USING PUBLICLY AVAILABLE  
SOFTWARE..... 8

IMSI CATCHERS CAN BE DETECTED BY MODIFYING POPULAR MOBILE PHONES  
THAT CAN BE PURCHASED FOR APPROXIMATELY \$20 ..... 9

THE PUBLIC INTEREST IS NOT SERVED BY CONTINUED SECRECY REGARDING IMSI  
CATCHERS ..... 10

CONCLUSION..... 11

## STATEMENT OF INTEREST OF *AMICI CURIAE*

*Amici* are experts and researchers with skills in the areas of computer science, privacy, security and surveillance:

- Jacob Appelbaum, Staff Research Scientist, Security and Privacy Research Lab, University of Washington
- David Burgess, co-founder and lead developer of the OpenBTS project
- Eric King, Human Rights and Technology Advisor, Privacy International
- Aaron Martin, PhD, Information Systems and Innovation Group, Department of Management, London School of Economics and Political Science
- Christopher Parsons, Doctoral Candidate, Political Science, University of Victoria
- Christopher Soghoian, Graduate Fellow, Center for Applied Cybersecurity Research, Indiana University
- Katrin Verclas, Director, MobileActive Corp

*Amici* submit this brief in their individual capacities. The affiliations listed are for identification purposes only.

## SUMMARY OF ARGUMENT

On the basis of *ex parte* testimony by the FBI, this court has concluded that disclosure of the techniques used by the government to locate the defendant would “hamper future law enforcement efforts by enabling adversaries of law enforcement to evade detection”<sup>1</sup> and “defeat electronic surveillance operations.”<sup>2</sup>

Although specific details regarding the mobile tracking device used by the government remain shrouded in secrecy, the government has at least conceded that the tracking technology simulated a cell site.<sup>3</sup> *Amici* seek to inform the court that a substantial amount of detailed technical information about cell site simulators and other related mobile phone surveillance technology is already public. Information about such tracking technology, commonly referred to as an IMSI catcher by surveillance experts, is revealed in multiple patent filings, academic research papers, and marketing materials from multiple surveillance technology vendors, many of whom are not shy about advertising their respective products.

Using this information and freely available software, security researchers have built their own IMSI catchers using widely available electronic equipment that can be purchased for

---

<sup>1</sup> Doc 723 at 20.

<sup>2</sup> Doc 723 at 12.

<sup>3</sup> Doc. 602 at 3.

approximately \$1500. Researchers have also developed and freely distributed software tools that detect the use of IMSI catchers and other mobile phone tracking technologies.

The government may wish that the public remain in the dark regarding its surveillance of mobile phones using IMSI catchers and specifically, details regarding how such surveillance technology can be detected and thwarted. That genie cannot be put back into the bottle. Detailed information about IMSI catchers, as well as software enabling the detection of such covert surveillance of mobile telephones, is already available to the public and accessible to anyone with access to an Internet search engine.

Finally, the communications privacy of millions of law-abiding Americans is already threatened by the use of this and similar interception technologies by non-US government entities, such as stalkers, criminals, and foreign governments engaged in espionage. As such, the public interest is best served by greater public discussion regarding these tracking technologies and the security flaws in the mobile phone networks that they exploit, not less.

## INTRODUCTION

The FBI has claimed that the make and model of the technology used to locate the defendant is “law enforcement sensitive, and pursuant to FBI policy, cannot be released to the general public.”<sup>4</sup> However, in public filings, the government has conceded that the mobile tracking device it used to locate the defendant simulated a cell site, that it mimicked a Verizon Wireless cell tower and sent signals to, and received signals from, the aircard allegedly used by the defendant.<sup>5</sup> The government has also acknowledged that signals sent by the mobile tracking device to the aircard allegedly used by the defendant would not have been sent to the aircard by Verizon in the normal course of operation of its own cell towers.<sup>6</sup>

Government investigators in this case used the term Stingray to describe the surveillance technology used to track the defendant.<sup>7</sup> The Harris Corporation markets cell site simulators under the Stingray brand. However, the government insists that Stingray is a generic term for a particular mobile surveillance technology.<sup>8</sup>

---

<sup>4</sup> Doc 674 at 1.

<sup>5</sup> Doc. 602 at 3.

<sup>6</sup> Doc. 644 at 3.

<sup>7</sup> USPIS Investigation Details Report Entry, USPIS Inspector James L. Wilson, August 7, 2008, cited by defendant in Doc. 483-3 at 29 (“On 7/16/08, we were informed that they were able to track a signal and were using a ‘Stingray’ to pinpoint the location of the aircard.”)

<sup>8</sup> Jenifer Valentino-DeVries, ‘Stingray’ Phone Tracker Fuels Constitutional Clash, Wall Street Journal, September 22, 2011, available at: <http://online.wsj.com/article/SB10001424053111904194604576583112723197574.html>

In addition to these public disclosures, FBI Supervising Agent Morrison also provided testimony in an *ex parte* hearing on December 14, 2011. On the basis that testimony, this court has concluded that disclosure regarding the techniques used by the government to locate the defendant would “hamper future law enforcement efforts by enabling adversaries of law enforcement to evade detection”<sup>9</sup> and “defeat electronic surveillance operations.”<sup>10</sup>

Due to the *ex parte* nature of the hearing, amici do not know what the court has been told by the government about the degree to which detailed information about IMSI catchers is already public. Likewise, although this court has ruled that disclosure of such information in this case would enable adversaries of law enforcement to evade detection, it is unclear if this court is aware that it is already possible for such surveillance technologies to be detected and thwarted using freely available software and easily modifiable commodity mobile phones.

### **IMSI CATCHERS HAVE BEEN SOLD BY COMMERCIAL SURVEILLANCE VENDORS FOR MORE THAN FIFTEEN YEARS**

The market for “off the shelf” surveillance technology, used by governments around the world, is now a \$5 billion annual business.<sup>11</sup> At industry trade shows held several times per year at locations around the world, hundreds of vendors show off the latest tracking, monitoring and eavesdropping technology to thousands of potential customers: law enforcement and intelligence agencies from around the world and the telecommunications providers who carry the private communications of their customers (and are often tasked with performing communications intercepts).<sup>12</sup> According to industry experts, the best-selling technology in the espionage community at present is mobile phone monitoring equipment, such as IMSI catchers.<sup>13</sup>

Although the surveillance industry has grown in recent years, IMSI catchers are not a new technology. Law enforcement and intelligence agencies have purchased and used commercial

---

<sup>9</sup> Doc 723 at 20.

<sup>10</sup> Doc 723 at 12.

<sup>11</sup> Jennifer Valentino-DeVries, How the ‘Off the Shelf’ Surveillance Industry Has Grown, Wall Street Journal, November 18, 2011, available at: <http://blogs.wsj.com/digits/2011/11/18/how-the-off-the-shelf-surveillance-industry-has-grown/>

<sup>12</sup> Sari Horwitz, Shyamantha Asokan and Julie Tate, Trade in surveillance technology raises worries, Washington Post, December 1, 2011, available at: [http://www.washingtonpost.com/world/national-security/trade-in-surveillance-technology-raises-worries/2011/11/22/gIQAFFZOGO\\_story.html](http://www.washingtonpost.com/world/national-security/trade-in-surveillance-technology-raises-worries/2011/11/22/gIQAFFZOGO_story.html)

<sup>13</sup> Stefan Krempel, 28C3: New attacks on GSM mobiles and security measures shown, The H Open, 28 December, 2011, available at: <http://www.h-online.com/open/news/item/28C3-New-attacks-on-GSM-mobiles-and-security-measures-shown-1401668.html>

IMSI catchers since at least the mid-1990s. This includes the FBI, which used cell site simulator tracking technology made by the Harris Corporation as early as 1995,<sup>14</sup> as well as the governments of Australia and Germany.<sup>15</sup>

In the United States, the Harris Corporation is perhaps the best-known manufacturer of IMSI surveillance equipment, particularly after a September 2011, front-page Wall Street Journal article that highlighted this case.<sup>16</sup> However, Harris is but one firm in a crowded industry, something that Harris has itself acknowledged in filings with the FCC.<sup>17</sup> IMSI catchers are made and sold by many other companies, some in the United States and others located in Europe, the Middle East and elsewhere.

## **SURVEILLANCE VENDORS PROUDLY ADVERTISE THEIR IMSI CATCHERS AND DESCRIBE THEIR FEATURES IN PUBLIC MARKETING MATERIALS**

Several surveillance vendors advertise their IMSI catcher products on their own websites, and include significant amounts of detailed technical information in marketing materials that they publicly distribute. These include NeoSoft AG (Switzerland),<sup>18</sup> Ability (Israel),<sup>19</sup> and View Systems (Maryland, USA).<sup>20</sup>

---

<sup>14</sup> Tsutomu Shimomura, *Catching Kevin*, *Wired*, February 1996, available at: [http://www.wired.com/wired/archive/4.02/catching\\_pr.html](http://www.wired.com/wired/archive/4.02/catching_pr.html) (“The team talked to me a little about the technology they had toted along in the station wagon, especially something called a cell-site simulator, which was packed in a large travel case. The simulator was a technician’s device normally used for testing cell phones, but it could also be used to page Mitnick’s cell phone without ringing it, as long as he had the phone turned on but not in use. The phone would then act as a transmitter that they could home in on with a Triggerfish cellular radio direction-finding system that they were using.”)

<sup>15</sup> See *MMI Research Ltd v Cellxion Ltd & Ors* [2009] EWHC 418 (Pat) (11 March 2009), available at <http://www.bailii.org/ew/cases/EWHC/Patents/2009/418.html> (describing the sale of an IMSI Catcher made by Rohde & Schwarz to the Australian government in April 1998 and summarizing several German government documents from 1997 revealing the use of IMSI catchers)

<sup>16</sup> Jenifer Valentino-DeVries, *'Stingray' Phone Tracker Fuels Constitutional Clash*, *Wall Street Journal*, September 22, 2011, available at: <http://online.wsj.com/article/SB10001424053111904194604576583112723197574.html>

<sup>17</sup> Tania W. Hanna and Evan S. Morris, *Final Request for Confidentiality of Harris Corporation for FCC ID No. NK731000176* (FCC Correspondence Number 39482), March 21, 2011, at page 2, archived at <http://files.cloudprivacy.net/harris-fcc.pdf> (“Harris competes with a number of companies that are developing and marketing similar public safety devices”)

<sup>18</sup> NeoSoft AG, *Portable IMSI/IMEI GSM catcher NS-17-1*, available at: [http://www.neosoft.ch/products/emerg\\_tracking/detail.php?ID=1017&IBLOCK\\_ID=39](http://www.neosoft.ch/products/emerg_tracking/detail.php?ID=1017&IBLOCK_ID=39) (“The Compact GSM Base

While not published on its own website, Bahia 21, a Maryland based surveillance vendor submitted a public comment to the Commerce Department, proudly advertising its own IMSI catcher technology for use detecting contraband phones in US prisons.<sup>21</sup>

In November and December 2011, the Wall Street Journal, WikiLeaks and Privacy International published hundreds of pages of product marketing materials from ISS World, one of the largest surveillance industry trade shows. These documents include several brochures describing IMSI catcher products in great technical detail from vendors that include MMI Research / Cobham (United Kingdom),<sup>22</sup> Elaman (Germany)<sup>23</sup> and Verint (Israel).<sup>24</sup>

---

unit forces GSM phones in its vicinity to register with it. Unlike others IMSI/IMEI catchers NS-17-1 does not need to transmit very powerful signals in order to force GSM phones to make the handover from the real GSM network into this micro network....The system ensures selection of subscribers (targets) according to known IMSI or/and IMEI identifications. Also, it has the means of detection of such identifications according to the results of statistical processing of a list of registered subscribers....The system operates invisibly, so that the mobile station subscriber is unable to detect it. The system does not interfere with the external mobile GSM networks.”)

<sup>19</sup> Ability, Active GSM Interceptor, available at: <http://www.interceptors.com/intercept-solutions/Active-GSM-Interceptor.html> (“The IBIS-II extracts easily and in short time the mobiles ID’s such as IMEI, IMSI & TMSI and allows the user in no time to identify his target mobiles and to monitor them. The IBIS-II offers a complete set of capabilities and advance features to allow the user to control the GSM environment and GSM communication. The user can control the level of service to the target mobiles, selectively Jam specific mobiles, perform silent calls, call or SMS on behalf of target mobile, change SMS messages ”on the fly”, detect change of SIM card or change of handset, and support Direction Finding system and many additional operational features.”)

<sup>20</sup> View Systems, Cell Phone Intercept Apparatus, [http://www.viewsystems.com/pdf/CIA\\_11\\_20\\_06.pdf](http://www.viewsystems.com/pdf/CIA_11_20_06.pdf) (“Full identification of IMSI, IMEI and TMSI information and dynamic control capabilities, including comprehensive denial of service...Optional SMS and “Man In the Middle” Voice decode/record and forward...Proprietary “TrueStealth” technology supports repatriation of original TMSI and GCI on most handsets. This allows for rapid information gathering to later use on a complimentary passive system, and also virtually eliminates the possibilities of being detected due to switch activity on the network.”)

<sup>21</sup> Bahia 21, RESPONSE to National Telecommunications Information Administration Notice of Inquiry (Docket # 100504212-0212-01) Requesting Information on Preventing Contraband Cell Phone Use in Prisons, June 11, 2011, available at <http://www.ntia.doc.gov/files/ntia/comments/100504212-0212-01/attachments/BAHIA21%20resposne%20to%20NTIA%20NOI.pdf> (“[C]overtly capture IMSI/IMEI data of 2G and 3G cell phones in range of the catcher inside the prison and to take any actions such as blocking incoming or outgoing calls Voice, Data, SMS), identifying origin and destination of calls, etc.”)

<sup>22</sup> M.M.I Research trading as Cobham Surveillance, Tactical Lawful Intercept, May 2009, available at [http://wikileaks.org/spyfiles/files/0/43\\_200906-ISS-PRG-COBHAM.pdf](http://wikileaks.org/spyfiles/files/0/43_200906-ISS-PRG-COBHAM.pdf) (Sales materials for this company state that when used, “incoming and outgoing target calls/SMS can be intercepted and will be automatically recorded.” It also states that “the system can override the call destination and redirect to a preferred number without the target knowing”, which it suggests is useful in a hostage situation.)

The FBI has assured this court that the “equipment used to locate the defendant’s aircard did not capture, collect, decode, view or otherwise obtain any content transmitted from the aircard.” The government has also informed this court that the FBI’s “equipment did not capture any content and it did not act as a ‘man in the middle,’ collecting data and passing it along to Verizon Wireless.”<sup>25</sup>

Although the specific equipment used by the FBI may have been configured to not intercept content, the publicly available marketing materials from surveillance vendors make it clear that one of the most basic features offered by commercial IMSI catchers is the ability to capture and intercept communications.

---

<sup>23</sup> [http://wikileaks.org/spyfiles/files/0/188\\_201106-ISS-ELAMAN3.pdf](http://wikileaks.org/spyfiles/files/0/188_201106-ISS-ELAMAN3.pdf) (“Active systems - Such systems simulate a GSM/UMTS base station to attract GSM/UMTS phones away from the normal GSM/UMTS network and log into the system’s ‘fake’ virtual base station. As soon as the phone is logged onto the more attractive active system, its identity is extracted (IMSI and IMEI). By logging the phone onto the virtual base station the phone can be forced to transmit on a given channel, frequency and time-slot (establishing a ‘silent call’). This transmission can be picked up by a direction finding system (vehicle based or handheld) which then gives the exact position of the target phone. When the target phone is logged into the active system intercepting of calls can be done, but only calls that are initiated by the target (target is out of the normal GSM/UMTS network so no calls can be received by the target phone). In addition, phones can be completely taken off the real network (‘intelligent jamming’), fake calls and SMS can be sent to the target phone, and private networking by using the virtual base station can be realized and the battery of the target phone can be drained, etc. The active system also allows operating within UMTS networks. Collecting the identity of the target phone (IMSI, IMEI) can be done without bringing the phone down to GSM/GPRS, therefore, no jamming of the overall UMTS signal is needed. For all other operations, such as locating the phone, intercepting, etc. the target UMTS phone is either pushed back into GSM mode by the system or new UMTS Direction Finders can be supplied for locating of UMTS phones only.”)

<sup>24</sup> Two pages of Verint promotional materials were originally included in [http://wikileaks.org/spyfiles/files/0/184\\_201106-ISS-AGNITIO.pdf](http://wikileaks.org/spyfiles/files/0/184_201106-ISS-AGNITIO.pdf), but subsequently removed. These two pages have been archived at <http://files.cloudprivacy.net.s3.amazonaws.com/wikileaks-verint-location-tracking.pdf> (“UMTS Location Finding – Used with the Verint proprietary homing device, Verint U-Com, ENGAGE G12 can effectively and precisely locate phones on UMTS networks. Housed in an inconspicuous bag and operated via a wireless PDA, the U-Com is a valuable addition for covert tracking operations....Advanced UMTS (3G) features – these advanced features, which include phone blocking, denial of service, precise distance range estimation and identity correlation, help government agencies identify and apprehend targets avoiding detection by switching their phones to 3G-only mode....Exceptional interception capabilities – the ENGAGE G12 Call and SMS interception module provides outstanding reliability and voice quality. Further, real-time SIM cloning enables undetectable interception of outgoing and incoming calls on all GSM encrypted networks, including A5/1 and A5/3.”)

<sup>25</sup> Doc 674 at 2.

## A SUBSTANTIAL AMOUNT OF DETAILED TECHNICAL INFORMATION ABOUT IMSI CATCHERS IS ALREADY PUBLIC

In 1999, Rohde & Schwarz, a German surveillance vendor filed for and later obtained a European patent on a “method for identifying a mobile phone user or for eavesdropping on outgoing calls.”<sup>26</sup> In 2005 and 2006, UK surveillance vendor M.M.I Research Ltd filed for several patents, including a method to “acquir[e] identity parameters by emulating base stations.”<sup>27</sup> These patent applications disclose a significant amount of detailed technical information, which, as patent laws require, enable someone reasonably skilled in the respective technical art to make or use the invention.<sup>28</sup>

Amici member David Burgess, a telephony expert who has written software for IMSI catchers has stated that “the most common way to build an IMSI-catcher comes directly from the [Rohde & Schwarz] patent itself and is based entirely on off-the-shelf commercial equipment. Nearly any BTS [(base transceiver station)] or BTS simulator can be used as the basis of an IMSI-catcher.”<sup>29</sup>

For more than a decade, computer security researchers and academics have written about the threat of IMSI catchers.<sup>30</sup> Some of these scholarly works include detailed, protocol-level information explanations of IMSI catcher interception.<sup>31</sup> Although much of this research has

---

<sup>26</sup> European Patent # 1051053 available at [http://ep.espacenet.com/e/publicationDetails/originalDocument?CC=EP&NR=1051053A2&KC=A2&FT=D&ND=5&date=20001108&DB=ep.espacenet.com&locale=en\\_EP](http://ep.espacenet.com/e/publicationDetails/originalDocument?CC=EP&NR=1051053A2&KC=A2&FT=D&ND=5&date=20001108&DB=ep.espacenet.com&locale=en_EP)

<sup>27</sup> Andrew Paul Pridmore et al., Acquiring Identity Parameters by Emulating Base Stations, U.S. Patent Application Publication number US 2008/0220749 A1, filed on July 17, 2006, Foreign application priority date, July 22, 2005, available at: <http://www.faqs.org/patents/app/20080220749>. See also Paul Maxwell Martin et al., Acquiring Identity Parameter, U.S. Patent Application Publication number 2009/0023424, filed on January 30, 2007, Foreign application priority date, January 31, 2006, available at: <http://www.faqs.org/patents/app/20090023424>

<sup>28</sup> See for example, *United States v. Teletronics, Inc.*, 857 F.2d 778, 785, 8 USPQ2d 1217, 1223 (Fed. Cir. 1988) (“The test of enablement is whether one reasonably skilled in the art could make or use the invention from the disclosures in the patent coupled with information known in the art without undue experimentation.”)

<sup>29</sup> David Burgess, Some Comments on IMSI-Catchers, *The OpenBTS Chronicles*, May 6, 2009, available at: <http://openbts.blogspot.com/2009/04/some-comments-on-imsi-catchers.html>

<sup>30</sup> Hannes Federrat, Protection in Mobile Communication, in: Günter Müller, Kai Rannenberg (Ed.): *Multilateral Security in Communications*, Addison-Wesley-Longman 1999, available at [http://epub.uni-regensburg.de/7382/1/Fede3\\_99Buch3Mobil.pdf](http://epub.uni-regensburg.de/7382/1/Fede3_99Buch3Mobil.pdf).

<sup>31</sup> See Daehyun Strobel, IMSI Catcher, Seminararbeit, Ruhr-Universität at Bochu, July 13, 2007, available at [http://www.emsec.rub.de/media/crypto/attachments/files/2011/04/imsi\\_catcher.pdf](http://www.emsec.rub.de/media/crypto/attachments/files/2011/04/imsi_catcher.pdf). See also Julian Dammann, IMSI-Catcher and Man-in-the-Middle attack, Mobile Security Seminar presentation, University of Bonn, February 9,

been published by experienced academic researchers,<sup>32</sup> undergraduate students have also written research papers that describe IMSI catchers in detail.<sup>33</sup>

## **IMSI CATCHERS CAN NOW BE BUILT FOR \$1500 USING PUBLICLY AVAILABLE SOFTWARE**

At the most basic level, an IMSI catcher is a cellular base station that is configured to broadcast the network country code and mobile network code of a commercial network operator (such as AT&T or T-Mobile). Thus, as one security expert has written, “anyone who has a device that can run as a GSM base station has the ability to run an IMSI catcher.”<sup>34</sup>

Several open-source software projects have been created by technologists and hobbyists in recent years, in order to lower the cost of running mobile telephone networks. Although these projects were not created for the purpose of enabling users to create their own IMSI catchers, by modifying a few configuration settings, it is possible to use one of these telephony tools to create an IMSI catcher.<sup>35</sup> One of these projects is OpenBTS, which was co-created by amici

---

2011, available at [http://cosec.bit.uni-bonn.de/fileadmin/user\\_upload/teaching/10ws/10ws-sem-mobsec/talks/dammann.pdf](http://cosec.bit.uni-bonn.de/fileadmin/user_upload/teaching/10ws/10ws-sem-mobsec/talks/dammann.pdf)

<sup>32</sup> Ulrike Meyer and Susanne Wetzel, 2004. A man-in-the-middle attack on UMTS, In Proceedings of the 3rd ACM workshop on Wireless security (WiSe '04), ACM, New York, NY, USA, available at <http://www.cs.stevens.edu/~swetzel/publications/mim.pdf>. See also Muxiang Zhang and Yuguang Fang, Security analysis and enhancements of 3GPP authentication and key agreement protocol, IEEE Transactions on Wireless Communications, March 2005, available at <http://www.fang.ece.ufl.edu/mypaper/tw05zhang.pdf>.

<sup>33</sup> See Jonathan Simon Arbib, Security Measures in GSM Networks and Possible Attack Methods, Senior Project in Computing, Richmond, the American International University in London, Spring 2008, available at <http://arbib.it/wp-content/uploads/2008/05/senior-dissertation-jonathan-arbib.pdf>. See also Daehyun Strobel, IMSI Catcher, *id*.

<sup>34</sup> Harald Welte, On the recent news items about the homebrew IMSI-catcher for 1500 USD, August 1, 2010, available at <http://laforge.gnumonks.org/weblog/2010/08/01/>.

<sup>35</sup> See *id* (“If a user choses to configure the NCC and MNC of a commercial operator and allow “unknown/unregistered/unprovisioned IMSIs (SIMs) on his network, he will effectively have an IMSI catcher.”) See also Stefan Kreml, 26C3: GSM hacking made easy, The H Open, 29 December, 2009, available at <http://www.h-online.com/open/news/item/26C3-GSM-hacking-made-easy-893245.html> (“OpenBTS and the free Asterisk software for telephone systems previously helped the security experts build a budget IMSI catcher for active attacks on GSM. While the equivalent devices, mainly used by the German police and intelligence agencies to locate mobile phone users, can be purchased for around 1500 US dollars, the open source solution provides an even more low-cost alternative, said Nohl.”)

member David Burgess. The OpenBTS software runs on a standard personal computer that is attached to a software-defined radio that can be purchased for approximately \$1500.<sup>36</sup>

In July 2010, a security researcher demonstrated an OpenBTS based IMSI catcher that masqueraded as an AT&T tower in front of thousands of attendees at Defcon, a computer hacker conference held each year in Las Vegas. Up to thirty phones were connected to the fake tower at any given time.<sup>37</sup> Although incoming calls could not be received, outgoing calls were transmitted and simultaneously recorded by the researcher, further demonstrating that IMSI catchers can be used for communications interception.<sup>38</sup>

## **IMSI CATCHERS CAN BE DETECTED BY MODIFYING POPULAR MOBILE PHONES THAT CAN BE PURCHASED FOR APPROXIMATELY \$20**

In December 2011, two prominent European security researchers released Catcher Catcher, a tool designed to “detect unusual network behavior caused by IMSI catchers and tracking attacks.”<sup>39</sup> The free, open-source software tool runs on several cheap, commonly available mobile phones that can be purchased for approximately \$20.<sup>40</sup> At least one these phones, the Motorola C139, has been distributed by Tracfone, a major U.S. prepaid wireless carrier, and sold at drug stores, mini marts and other retailers nationwide.

The Catcher Catcher tool observes mobile phone network activity, looking for “behavior different from normal base stations” (these are the towers operated by the phone companies).<sup>41</sup> The

---

<sup>36</sup> See OpenBTS, available at <http://openbts.sourceforge.net/>. See also Andreas Steil, Introduction (OpenBTS), available at <http://www.fh-kl.de/~andreas.steil/Projekte/OpenBTS/index.html>. See also Ettus Research LLC, USRP Family, available at <http://www.ettus.com/products> (listing several software defined radios used by OpenBTS).

<sup>37</sup> Kelly Jackson Higgins, Researcher Intercepts GSM Cell Phones During Defcon Demo, Dark Reading, July 31, 2010, available at: <http://www.darkreading.com/security-services/167801101/security/attacks-breaches/226500010/researcher-intercepts-gsm-cell-phones-during-defcon-demo.html>

<sup>38</sup> Andy Greenberg, Despite FCC "Scare Tactics," Researcher Demos AT&T Eavesdropping, Forbes, July 31, 2010, available at: <http://www.forbes.com/sites/firewall/2010/07/31/despite-fcc-scare-tactics-researcher-demos-att-eavesdropping/>

<sup>39</sup> Catcher Catcher, available at <http://opensource.srlabs.de/projects/catcher>.

<sup>40</sup> A list of the cell phones that work with the Osmocom can be found here: <http://bb.osmocom.org/trac/>

<sup>41</sup> These suspicious behaviors include, connecting to a base station with no encryption, when encryption was used with the same operator in the past, receiving “silent” text messages, or the target’s phone transmitting at the highest possible power. A list of the suspicious network behaviors are available at: <http://opensource.srlabs.de/projects/catcher/wiki/Wiki>

software distinguishes between three different modes: the first displays “an indication that you might have been caught”; the second, “a very strong indication”; while the third tells the user, “You are being tracked down; throw away your phone and run.”<sup>42</sup>

On December 27, 2011, the researchers demonstrated this tool in front of a large audience at the Chaos Communications Congress, a major computer security conference in Berlin, Germany.<sup>43</sup>

## **THE PUBLIC INTEREST IS NOT SERVED BY CONTINUED SECRECY REGARDING IMSI CATCHERS**

In oral arguments before this court, the government has claimed that “the sensitive nature of the equipment [used to locate the defendant] goes beyond issues of law enforcement to matters of national security” as “some of this equipment is not only used in the law enforcement realm, it's used in the national security realm.”<sup>44</sup>

The government is indeed correct in stating that there are significant national security issues associated with IMSI catchers and other forms of mobile surveillance technology. However, the most important of these national security concerns are not related to the use of IMSI catchers by the US government, but by foreign intelligence agencies in the United States.

The US government and its intelligence agencies do not have a monopoly on the use of IMSI catchers. Surveillance vendors sell these and similar products around the world, to governments that are allied with ours, as well as those that are on less than friendly terms. An IMSI catcher, when used in Washington DC, New York, or San Francisco can intercept the communications of politicians, bankers and technology executives, regardless of who owns the surveillance device – the FBI, a local sheriff's department, a foreign intelligence agency, or a tech-savvy criminal.

IMSI catchers abuse security flaws in the decades-old protocols still used by our wireless phone networks. As these flaws remain unfixed, the phone calls of millions of Americans can now be easily snooped on by anyone nearby with \$1500 worth of equipment and some software that can be freely downloaded from the Internet. As such, the public interest is not served by continued secrecy regarding this critical vulnerability in our communications network.

---

<sup>42</sup> *Id.*

<sup>43</sup> See: Karsten Nohl and Luca Melette, Defending mobile phones, Chaos Communications Congress, December 27, 2011, video of talk and slides available at: <http://events.ccc.de/congress/2011/Fahrplan/events/4736.en.html>.

<sup>44</sup> Doc 451 at 14.

## CONCLUSION

On the basis of *ex parte* testimony by the government, this court has concluded that disclosure regarding the techniques used by the government to locate the defendant would “hamper future law enforcement efforts by enabling adversaries of law enforcement to evade detection”<sup>45</sup> and “defeat electronic surveillance operations.”<sup>46</sup>

Once a surveillance technology has been patented, studied by academic experts, and described in depth by undergraduate students, it is no longer a secret, even if the government wishes otherwise. Likewise, now that any hobbyist can build one for less than \$1500, governments no longer even have a monopoly on their use.

As the recent public release of the Catcher Catcher tool demonstrates, there is more than enough public information about this and other similar surveillance technologies for researchers to build privacy-enhancing tools to detect and thwart their use. As much as the government may wish that this information not be public, it is already out, and available to anyone with an Internet search engine.

Furthermore, as the US government neither has, nor can it enforce a monopoly for itself over the use of IMSI catchers, the public interest is not served by the government’s continued secrecy regarding its use of this surveillance technique. Rather than urging this court to prevent the public from learning more about its use of IMSI catchers, the government should be taking steps to protect the communications of innocent Americans from the real threat of IMSI catchers used by foreign governments and criminals.

Dated: January 17, 2012

By: \_\_\_\_\_  
Katrin Verclas  
(*pro se*)

Director,  
MobileActive Corp  
121 W 27<sup>th</sup> Street, Suite 702  
New York, NY 10001

Email: [katrin@mobileactive.org](mailto:katrin@mobileactive.org)

---

<sup>45</sup> Doc. 723 at 20.

<sup>46</sup> Doc. 723 at 12.