Modern Safeguards for Modern Surveillance: An Analysis of Innovations in Communications Surveillance Techniques

GUS HOSEIN* & CAROLINE WILSON PALOW†

TABLE OF CONTENTS

I. INTRODUCTION

To understand communications surveillance law is to try to resolve the three-body problem of simultaneously comprehending law, policy, and technology while at least two of the three may be changing at any moment in time. This makes it one of the more exciting domains for scholars, analysts, and technologists, but it is also one of the most challenging.

Communications surveillance is a rapidly shifting landscape from the perspectives of policy and technology. Governments across the world are deploying new techniques and technologies with alarming speed. We are achieving new levels of surveillance, quickly approaching what Justice Brandeis warned about when he said that "[s]ubtler and more far-reaching means of invading privacy have become available to the Government," and that

* Gus Hosein is the Executive Director of Privacy International.
† Caroline Wilson Palow is a Legal Officer at Privacy International.

"[d]iscovery and invention have made it possible for the Government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet."[1] There is a rapidly growing market in communications surveillance technologies that can conduct surveillance in ways that just ten years ago were well beyond the limits of our technology and often our imaginations.

With widespread innovations in policy and technology across the world, what is most surprising is how old-fashioned our legislation is, and in turn, our safeguards. Many communications surveillance laws were drafted in the 1980s and 1990s, with updates in the 1990s and early 2000s.[2] Many countries across the world are still introducing laws on communications surveillance, but their models are quite old, often borrowing language from laws from the 1990s (in the case of U.S. and UK law) and international conventions such as the Council of Europe Cybercrime Convention of 2001.[3] They all ban interception of communications content, grant exceptions to government agencies, permit access to information about the communications (so-called communications metadata), establish authorization and oversight regimes, and permit government to order communications service providers to provide capabilities for lawful intercept and/or access.[4] But they are not keeping pace with the new forms of advanced surveillance techniques and policies being deployed.

In this Article we will draw out the modern landscape of surveillance policy and technologies (Part I). The deployment of new techniques and technologies is being done without new legal frameworks, and as such, we must resort to relying on older frameworks that may be unable to understand these new

---

[1] Olmstead v. United States, 277 U.S. 438, 473 (1928) (Brandeis, J., dissenting).

[2] *See, e.g.*, Electronic Communications Privacy Act (ECPA) of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.) (amending and updating Title III of the Omnibus Crime Control and Safe Streets Act of 1968, commonly called the Wiretap Act); Communications Assistance for Law Enforcement Act (CALEA) of 1994, Pub. L. No. 103-414, 108 Stat. 4279 (codified at 47 U.S.C. §§ 1001–1010 (2012)) (further amending the Wiretap Act and Stored Communications Act in 1994); Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT ACT) of 2001, Pub. L. No. 107-56, 115 Stat. 272 (codified in scattered sections of the U.S.C.) (further amending the Wiretap Act and Stored Communications Act); Interception of Communications Act (IOCA), 1985, c. 56 (Eng.) (regulating the interception of communications); Regulation of Investigatory Powers Act (RIPA), 2000, c. 23 (Eng.) (replacing IOCA); Telecommunications (Interception Capability) Act 2004 (Act No. 19/2004) (N.Z.); Loi relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées of June 30, 1994, MONITEUR BELGE [M.B.] [Official Gazette of Belgium], Jan. 24, 1995, 01542.

[3] Council of Europe Convention on Cybercrime, Nov. 23, 2001, E.T.S. No. 185, *available at* http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

[4] *See, e.g.*, Wire and Electronic Communications Interception and Interception of Oral Communications (Wiretap Act), 18 U.S.C. §§ 2510–2522 (2012); RIPA, 2000, c. 23; Telecommunications Act, 2004 (N.Z.); Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 § 5 (S. Afr.).

techniques, or constitutional safeguards that have a long and troubled history with innovation (Part II). Using the example of the lack of legislative activity in the United States, we look at how lower courts are trying to resolve the Fourth Amendment concerns inherent in some of these techniques, and make suggestions regarding how we believe current law should be applied (Part III).

We are in a moment of great uncertainty characterized by the absence of legislative activity implementing real safeguards, use of new communications surveillance capabilities often in secretive ways, and courts grappling to understand new technologies. Laws, technologies, and the courts have, until now, maintained a delicate balance on communications surveillance; when new technologies posed new threats, often the courts or the legislative bodies would respond. If one branch failed, another would usually pick up the gauntlet. After the U.S. Supreme Court decided that interception of communications did not qualify as a search under the Fourth Amendment in 1928,[5] Congress responded in the 1930s with strict controls.[6] In the 1960s the Supreme Court and Congress fed off one another to develop jurisprudence[7] and legislation.[8] Responding to abuses in the 1970s, Congress enacted new laws,[9] and when the Supreme Court decided against protecting certain metadata,[10] Congress responded with rules on "trap and trace" and "pen registers."[11] Unfortunately, we are currently seeing a lack of interest in safeguards from Congress and other legislatures around the world, while technical capabilities are expanding. There is even speculation that the Foreign Intelligence Security Court is being activist in enabling surveillance.[12] It is high time to reintroduce safeguards into the conversation, and to apply them against technologies that are increasingly used to conduct directed and mass surveillance of our sensitive information.

A. *A Brief History of Communications Surveillance*

Communications surveillance is almost as old as our ability to communicate.[13] While our attempts to regulate that surveillance are more recent, they still lag behind the pace of technological innovation. Scholars thus

---

[5] *Olmstead*, 277 U.S. at 464.

[6] *See* Communications Act of 1934, Pub. L. No. 416, 48 Stat. 1064 (codified as amended in scattered sections of 47 U.S.C.).

[7] *See, e.g.*, Katz v. United States, 389 U.S. 347 (1967).

[8] *See* Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197 (codified as amended at 18 U.S.C. §§ 2510–2522 (2012)) (containing Title III, commonly referred to as the Wiretap Act).

[9] *See* Foreign Intelligence Surveillance Act (FISA) of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended in scattered sections of 50 U.S.C.).

[10] *See* Smith v. Maryland, 442 U.S. 735, 745–46 (1979).

[11] *See* ECPA of 1986, Pub. L. No. 99-508, 100 Stat. 1868.

[12] *See* Eric Lichtblau, *In Secret, Court Vastly Broadens Powers of N.S.A.*, N.Y. TIMES, July 7, 2013, at A1.

[13] For a history of communication surveillance going back to the Egyptians, see generally DAVID KAHN, THE CODEBREAKERS: THE STORY OF SECRET WRITING (1967).

struggle to understand how to resolve modern forms of communications surveillance with older legal frameworks. For instance, our abilities to comprehend what a constitutional statement about a right to privacy actually means may be linked with the state of surveillance at the time.

Efforts to monitor communications are of course linked to our methods of communicating. With letters and post came the interception of postal communications. With the advent of property rights, people kept their received written communications at home, and these could be seized upon entry.[14] Communications within the home, in the form of interactions with other people, required secret surveillance through informants, and with technological innovation—bugs.[15] Intercepting packages and letters gave way to requiring telegraph offices to monitor communications, or more directly tapping wires. This was repeated with telephones, involving the actions of operators, or directly tapping the wire, or installing listening devices at one end.[16]

Much of the modern debate about communications surveillance focuses on the institutions implicated in such monitoring. Historically, in many countries, the government, or monopolies with close ties to the government, ran the postal services; and this often continued into the telegraph era.[17] As a result, the government didn't necessarily need to pass laws to compel a company to comply with interception requests because these companies were operating at the mercy of the government, even as an arm of the government. The telephone system was operated for the most part in a similar way to the telegraph and the post: a limited number of companies or a government agency responsible for administering the service, which could also be responsible for administering surveillance.[18]

Market innovations created policy challenges in this system, leading to policy change. As the industry of communications service provision became more diverse, whether by deregulation of telephone services or through the rise of mobile phone services, the relationships with governments became more complicated. Companies without pre-existing relationships with governments sought legislative cover for helping governments with surveillance. Equally,

---

[14] Entick v. Carrington, (1765) 95 Eng. Rep. 807 (K.B.).

[15] *See* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 572 (2009).

[16] The *Katz* case in 1967, though famously known for its comments on interception of communications, was actually a case of placing a listening device in a telephone booth. Katz v. United States, 389 U.S. 347, 348 (1967).

[17] For an interesting historical note about Lincoln's ability to monitor all telegraphic activity in the United States during the Civil War, see generally David T.Z. Mindich, *Lincoln's Surveillance State*, N.Y. TIMES, July 6, 2013, at A17.

[18] For an interesting history of surveillance of telecommunications in the United Kingdom, see Malone v. United Kingdom, App. No. 8691/79, 7 Eur. H.R. Rep. 14, 18–35 (1984). For a list of the national security agreements between the United States and telephone and cable companies, see *U.S. Government Foreign Telecommunications Providers Network Security Agreements*, PUB. INTELLIGENCE (July 9, 2013) [hereinafter PUB. INTELLIGENCE], http://publicintelligence.net/us-nsas.

companies who were identified publicly for closely cooperating with governments sought legal protections for having done so.[19] With the rise of human rights and civil liberties concerns, we saw the emergence of laws on communications surveillance, providing a legal basis for monitoring.

These laws were not being drafted just to provide privacy safeguards and legal cover. While they initially may have regulated snooping, eventually these laws shifted towards enabling surveillance programs. Policy developments leading to the Communications Assistance for Law Enforcement Act in the United States in the early 1990s, and many laws across the world in the late 1990s and early 2000s, focused on developing interception capabilities: requiring companies to provide access to communications, without regard to the technologies.[20] Wire "tapping" was no longer a reasonable way for gaining access to communications content because of the increased sophistication of telecommunications systems; and Internet communications couldn't be "intercepted" in the same way. As a result, governments mandated that companies could be ordered to provide access to communications content.[21]

In the early to mid-2000s, new programs emerged to ensure capture of communications metadata. Information about who is communicating with whom and when is generated as a by-product of transferring communications content. This data may reside in logs held at service providers, or may be embedded within the communications content. The ability of governments to gain access to this information also changed with the shift in technologies and the market. In the earlier phases of telephone communications, gaining access to this information required the use of "trap and trace" and "pen register" technologies at telephone companies.[22] With changes in billing, technologies capturing this information became relevant to the companies themselves; so the policy focus turned to providing government access to these logs. But companies may not necessarily keep these logs for as long as governments want, and in the early to mid-2000s governments began introducing "data

---

[19] The Protect America Act of 2007 provided for retroactive immunity for companies, out of a concern that "the private sector might be unwilling to cooperate with lawful Government requests in the future without unnecessary court involvement and protracted litigation." White House Office of Commcn's, *Retroactive Liability Protection Is Critical to Our National Security*, U.S. DEP'T JUSTICE (July 8, 2008), http://www.justice.gov/archive/ll/docs/fisa-factsheet-070808.pdf. The FISA Amendments Act made this immunity permanent. For a historical example, see the history of Operation Shamrock from the 1940s, under which the executives of ITT, RCA, and Western Union agreed to cooperate with the U.S. Government in exchange for protections against prosecution. JAMES BAMFORD, THE SHADOW FACTORY: THE ULTRA-SECRET NSA FROM 9/11 TO THE EAVESDROPPING ON AMERICA 165–68 (2008).

[20] *See* Council Resolution (EC) No. 96/C of 17 Jan. 1995 O.J. (C 329) 2; RIPA, 2000, c. 23 (Eng.) (replacing IOCA); Telecommunications (Interception Capability) Act 2004 (Act No. 19/2004) (N.Z.); Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 § 5 (S. Afr.).

[21] *See* sources cited *supra* note 20.

[22] *See infra* text accompanying notes 164–66.

retention" laws, requiring companies to keep these logs for extended periods of time.[23]

Up until this point, access to communications content and metadata (hereafter "communications surveillance") was for the most part targeted. Due to resource limitations, in that we didn't have enough ears to listen to enough conversations, monitoring was limited to specific individuals or groups. As the communications infrastructure became more complex, new communications companies stepped in that didn't have the same old relationships with governments, the rate of communications increased, and they became increasingly digital. Surveillance arguably became more challenging for governments after years of gaining access to more information. New programs were developed, alongside new powers and new technologies, permitting less targeted approaches to communications surveillance.[24] Where previously an intelligence agency could be overwhelmed trying to monitor the communications of vast groups of people, we are now seeing that intelligence agencies have been monitoring the communications metadata of entire populations[25] and tapping the fiber optic cables that connect continents to gain direct access to data flows.[26] As these resource limitations were being erased, some laws were being changed to accommodate this new approach.[27]

---

[23] See Council Directive 2006/24, art. 1, 2006 O.J. (L 105) 54, 56 (EC) on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Council Directive 2002/58/EC; *see also* A. Michael Froomkin, *"PETs Must Be on a Leash": How U.S. Law (and Industry Practice) Often Undermines and Even Forbids Valuable Privacy Enhancing Technology*, 74 OHIO ST. L.J. 965, 977–78 (2013).

[24] Jane Mayer, *The Secret Sharer: Is Thomas Drake an Enemy of the State?*, NEW YORKER, May 23, 2011, http://www.newyorker.com/reporting/2011/05/23/110523fa_fact_mayer.

[25] *See, e.g.*, Jacques Follorou & Franck Johannès, *In English: Revelations on the French Big Brother*, SOCIÉTÉ (July 4, 2013), http://www.lemonde.fr/societe/article/2013/07/04/revelations-on-the-french-big-brother_3442665_3224.html; Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN, June 5, 2013, http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

[26] *See* Ewen MacAskill et al., *GCHQ Taps Fibre-Optic Cables for Secret Access to World's Communications*, GUARDIAN, June 21, 2013, http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa (reporting that the UK's spy agency, GCHQ, accesses undersea fiber optic cables to obtain communications); *NSA Slides Explain the PRISM Data-Collection Program*, WASH. POST, July 10, 2013 [hereinafter *PRISM Data-Collection*], http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/ (including a slide that highlights "[c]ollection of communications on fiber cables and infrastructure as data flows past").

[27] FISA was amended in 2008 to include a new, broad provision allowing for the collection of information regarding non-U.S. persons outside of the United States. *See* 50 U.S.C. § 1881a (2012). In order to undertake such monitoring, U.S. intelligence agencies need not specify the person or premises they intend to target. Instead, they merely must assure the secret Foreign Intelligence Surveillance Court that a significant purpose of the surveillance will be to obtain foreign intelligence information and that U.S. persons will not be intentionally targeted. *Id.*

The value of communications surveillance increased dramatically in this time as well. More of our societal interactions took place over and through modern communications infrastructure, sometimes without our knowledge. If we carry a mobile phone, our mobile network provider logs our locations; more of our interactions with friends, families, and colleagues results in a log, and increasingly a stored communication.[28] The sensitivity of this data has increased. Whereas previously metadata was often dismissed as being low value information,[29] it now constitutes information about everyone we've known, every place we've been, every item we've read, every information resource we've been interested in; and can be used to derive information about our present and future conduct.[30]

Interestingly, in 1928, when the Supreme Court was considering the *Olmstead* case, telephone companies apparently urged the Court to rule that government should not conduct wiretapping.[31] Professor Orin Kerr assumes that this was to encourage customers to use the telephone and keep government from interfering with their networks.[32] Now we are dealing with situations where so many requests are received that companies have developed web interfaces to give law enforcement agents direct access.[33] And these communications technologies are so ubiquitous that if people were not to use them, they would be socially and economically excluded.

We are also seeing another era of policy innovation. The building of monitoring capabilities into technologies, and the compulsion to cooperate and even retain information are no longer considered sufficient as communications may cross borders. Older laws compelling government access failed to consider cross-jurisdictional Internet communications (or actively excluded them).[34] Instead, they presumed citizens would communicate using telephone services provided by domestic companies. Even if they did consider email, they presumed that domestic companies were providing email services. Now communications between two citizens of a single country are likely to involve service providers in other countries.[35] It is more difficult for a government to

---

[28] VIKTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK 151 (2013).

[29] This is separate to the legal treatment, to be discussed in Part II.

[30] See, as examples, a review of Sandy Petland's work, Kate Greene, *TR10: Reality Mining*, MIT TECH. REV. (Mar.–Apr. 2008), http://www2.technologyreview.com/article/409598/tr10-reality-mining/, and also see Alberto Escudero-Pascual & Ian Hosein, *Questioning Lawful Access to Traffic Data*, 47 COMM. ACM 77, 81 (2004).

[31] Kerr, *supra* note 15, at 598.

[32] *Id.*

[33] Stephanie K. Pell & Christopher Soghoian, *Can You See Me Now?: Toward Reasonable Standards for Law Enforcement Access to Location Data That Congress Could Enact*, 27 BERKELEY TECH. L.J. 117, 121 (2012).

[34] *See* 47 U.S.C. § 1002(b)(2) (2012) (assistance capability requirements, excludes information services and private networks, long assumed to refer to the Internet).

[35] For instance, in 2012, Google stated it had 425 million active Gmail users worldwide. *See* Dante D'Orazio, *Gmail Now Has 425 Million Active Users*, VERGE (June 28,

reach into these foreign jurisdictions and to establish relationships with every company.

Since the mid-2000s, democratic governments have been proposing new policies to resolve this dilemma. One such policy is to require domestic service providers to actively collect information on all users' activities. Whereas previously providers were asked to grant access to content on a targeted basis, and to *retain* collected metadata on an untargeted basis, domestic communications carriers, such as providers of cable services, are now being asked to monitor all information that flows through their infrastructure in order to determine what people are doing on communications services in other countries. For instance, currently, in order for the British police to monitor who is emailing whom on Google they must go through the arduous process of getting Google in California to respond.[36] Instead, the British government has proposed requiring all Internet service providers in the UK to monitor all interactions by all Internet users to identify the activities of UK-based users of foreign service providers, to collect and retain the information on who is communicating with whom, when, and where.[37] When originally introduced in the UK, it was proposed that the national intelligence agency would store all this information. This policy was rejected.[38] But we are now realizing that the centralized storage of communications metadata, even for Internet services, is already occurring in some other countries, including the United States[39] and India.[40]

2012, 1:26 PM), http://www.theverge.com/2012/6/28/3123643/gmail-425-million-total-users. With Google's servers located in the United States and a handful of other countries, it is likely most of those users' communications are at some point routed outside of their country of origin. *See Data Center Locations*, GOOGLE, http://www.google.co.uk/about/data centers/inside/locations/index.html (last visited Aug. 12, 2013). *See generally* Dennis Hirsch, *In Search of the Holy Grail: Achieving Global Privacy Rules Through Sector-Based Codes of Conduct*, 74 OHIO ST. L.J. 1029 (2013).

[36] This can be through voluntary measures, or through Mutual Legal Assistance Treaties. *See, e.g.*, *Transparency Report: User Data Requests*, GOOGLE, http://www.google.com/transparencyreport/userdatarequests/legalprocess/ (last visited Aug. 28, 2013).

[37] *See* INTELLIGENCE & SEC. COMM., ACCESS TO COMMUNICATIONS DATA BY THE INTELLIGENCE AND SECURITY AGENCIES, 2013, Cm. 8514, ¶ 58 (U.K.) [hereinafter ACCESS TO COMMUNICATIONS DATA], *available at* http://www.official-documents.gov.uk/document/cm85/8514/8514.pdf.

[38] Press Release, Liberty (Nat'l Council for Civil Liberties), Liberty Welcomes Government Climb-Down on Centralised Communications Database (Apr. 27, 2009), *available at* http://www.liberty-human-rights.org.uk/media/press/2009/liberty-welcomes-government-climb-down-on-centralised-communications.php. The Mastering the Internet programme, however, was established around the same time as this "climb-down." Christopher Williams, *Jacqui's Secret Plan To "Master the Internet,"* REGISTER (May 3, 2009), http://www.theregister.co.uk/2009/05/03/gchq_mti/.

[39] *See, e.g.*, Press Release from James R. Clapper, Dir. Nat'l Intelligence, DNI Statement on Recent Unauthorized Disclosures of Classified Information (June 6, 2013), *available at* http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/868-dni-statement-on-recent-unauthorized-disclosures-of-classified-information?tmpl=

Another emerging policy is to allow governments to gain access through other means to information resources in other countries. Put simply, governments are seeking to conduct searches across borders, even if this involves the malicious hacking of computers in other jurisdictions. The Dutch Government is proposing a law that will allow the police to break into computers and mobile phones, both within the Netherlands and abroad, in order to install spyware and search and destroy data.[41] The Council of Europe has recently proposed action in this area, seeking to develop a Draft Protocol to its Cybercrime Convention to permit cross-border searches.[42]

Safeguards are rarely mentioned as governments introduce these new policies. In fact, these policies are not always openly discussed. Meanwhile technological innovations make even more new and diverse forms of communications surveillance possible.

---

component&format=pdf (confirming the United States is collecting and maintaining records of the information described in the leaked Verizon court order).

[40] See the analysis from The Centre for Internet & Society, Maria Xynou, *India's "Big Brother": The Central Monitoring System (CMS)*, CENTRE FOR INTERNET & SOC'Y (Apr. 8, 2013), http://www.cis-india.org/internet-governance/blog/indias-big-brother-the-central-monitoring-system. Subsequent reporting includes *India: New Monitoring System Threatens Rights*, HUM. RTS. WATCH (June 7, 2013), http://www.hrw.org/news/2013/06/07/india-new-monitoring-system-threatens-rights; Dhruva Jaishankar, *Beyond Snowden: US Surveillance System a Useful Model for Democratic, Terror-Hit India*, ECON. TIMES (June 27, 2013, 2:07 AM), http://economictimes.indiatimes.com/opinion/comments-analysis/beyond-snowden-us-surveillance-system-a-useful-model-for-democratic-terror/hit-India/articleshow/20788044.cms; Srikant Jayanthan, *Central Monitoring System Put Off till December, Telecom Test Lab to October*, ECON. TIMES (June 21, 2013, 4:27 AM), http://articles.economictimes.indiatimes.com/2013-06-21/news/40119215_1_national-telecom-policy-telecom-network-telecom-equipment.

[41] *Dutch Police May Get Right To Hack in Cyber Crime Fight*, BBC NEWS (May 2, 2013), http://www.bbc.co.uk/news/world-europe-22384145; Door Ton Siedsma, *Dutch Hacking Proposal Puts Citizens at Risk*, BITS FREEDOM (May 2, 2013, 12:51 PM), https://www.bof.nl/2013/05/02/dutch-hacking-proposal-puts-citizens-at-risk/.

[42] In June 2013, the Council of Europe hosted a meeting of civil society and industry to consult on the proposal. A useful summary is provided by EDRi in its EDRi-gram 11.11 of June 5, 2013 in *Transborder Data Access: Strong Critics on Plans To Extend CoE Cybercrime Treaty*, EDRI (June 5, 2013), http://www.edri.org/edrigram/number11.11/transborder-data-access-cybercrime-treaty. The current convention in article 32(b) already states that one government (a Party)

> may, without the authorisation of another Party, access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

Id. The Council of Europe is consulting on a draft protocol that would remove the requirement that a computer system be "in its territory." The authors have been in communication with the U.S. Department of Justice regarding these consultations.

B. *Modern Communications Surveillance Techniques*

Surveillance policies and surveillance technologies are intertwined. The adoption of the telephone required the development of "wire tapping" techniques. When telephony grew more advanced, industry was enticed through subsidies[43] and standards[44] to develop the capability for government to monitor communications. Mobile telecommunications and digital communications, particularly those involving the Internet, required new interception innovations to match the previous capabilities of government programs, and to match new ambitions.

Over the past two years, privacy advocates and journalists have been investigating the modern surveillance technology industry. Through attending trade shows and conducting other investigations, we have collectively uncovered a significant market in new techniques of communications surveillance.[45]

We have identified at least three types of communications surveillance technologies that are now being developed by companies and deployed in various cities and countries around the world.

1. *Targeted Use of Offensive Technologies*

Rather than conducting searches of computers and mobile phones upon seizure, through the use of surveillance backdoors and vulnerabilities the users of these technologies are able to gain access to a device, whether a computer or a smartphone, through surreptitious means, often at a distance. Using vulnerabilities in our operating systems and applications, these systems then enable governments to monitor all activities on the device, including all keystrokes;[46] and to execute commands including conducting searches of

---

[43] CALEA created a $500 million fund to help American telecommunications companies make their switches wiretap ready. OFFICE OF THE INSPECTOR GEN., U.S. DEP'T OF JUSTICE, THE IMPLEMENTATION OF THE COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT: AUDIT REPORT, at i (2006), *available at* http://www.justice.gov/oig/reports/FBI/a0613/final.pdf. The funds had been spent by 2002, though the FBI estimated in 2006 that only ten to twenty percent of the wireline switches, and approximately fifty percent of the pre-1995 and ninety percent of the post-1995 wireless switches, respectively, have CALEA software activated and thus are considered CALEA-compliant. *Id.* at 97–98.

[44] At the same time as CALEA was being finalized, the European Union in 1995 developed a resolution calling for lawful intercept standards. Council Resolution (EC) No. 96/C of 17 Jan. 1995 O.J. (C 329) 2 (on the lawful interception of telecommunications). The European Telecommunications Standards Institute subsequently developed these standards which are now built into European telecommunications technology.

[45] *See generally* Sari Horwitz, Shyamantha Asokan & Julie Tate, *Trade in Surveillance Technology Raises Worries*, WASH. POST, Dec. 1, 2011, http://articles.washingtonpost.com/2011-12-01/world/35286192_1_surveillance-technology-first-trade-show-products.

[46] This is akin to the technique used in the case of *United States v. Scarfo*, 180 F. Supp. 2d 572, 574 (D.N.J. 2001). However, that case involved surreptitious physical access to the

material on the devices, and turning on microphones and cameras. Some of the leading systems are developed by Gamma International[47] and Hacking Team.[48]

2. *Targeted and Semi-targeted Use of Mobile Phone Surveillance*

Rather than targeting mobile phone communications by approaching telephone network providers, it is possible to actively monitor mobile communications in the field. This is commonly done by using a device that impersonates a high priority base station for mobile communications. These devices can be small enough to be carried around[49] or even affixed to a drone. One implementation of this technique is commonly referred to as an "IMSI catcher."[50] By impersonating a base station, all mobile phones on that network in that area will connect to the monitoring device rather than the legitimate network. The device can therefore identify all phones within range. In a more advanced implementation, they can also enable direct access to communications content and metadata by routing calls through the base station. Key providers include Cobham PLC, NeoSoft AG,[51] Ability,[52] and View Systems.[53]

---

office of Scarfo using a search warrant, and the use was limited to identifying the password to a specific resource, an encrypted file. *Id.* The case was not appealed.

[47] FinFisher control servers have been found in Australia, Bahrain, Bangladesh, Brunei, Canada, Czech Republic, Estonia, Ethiopia, Germany, India, Indonesia, Japan, Latvia, Malaysia, Mexico, Mongolia, Netherlands, Qatar, Serbia, Singapore, Turkmenistan, United Arab Emirates, United Kingdom, United States, and Vietnam. MORGAN MARQUIS-BOIRE ET AL., THE CITIZEN LAB, YOU ONLY CLICK TWICE: FINFISHER'S GLOBAL PROLIFERATION 1 (2013), *available at* https://citizenlab.org/wp-content/uploads/2013/07/15-2013-youonly clicktwice.pdf.

[48] Hacking Team's technology has been implicated in the surveillance of Mamfakinch, a journalist collective in Morocco. MORGAN MARQUIS-BOIRE, THE CITIZEN LAB, BACKDOORS ARE FOREVER: HACKING TEAM AND THE TARGETING OF DISSENT? 1 (2012), *available at* https://citizenlab.org/wp-content/uploads/2012/10/12-2012-backdoorsarefor ever.pdf.

[49] Some companies sell a "wearable" form of the technology.

[50] An International Mobile Subscriber Identity is a unique identifier that is carried on the phone or in the SIM card (depending on the network) and is sent to the network for connectivity.

[51] NEOSOFT, CATALOGUE 2009: SYSTEMS 9–10 (2009), *available at* http://www.neo soft.ch/support/download/catalog_systems.pdf ("The Compact GSM Base 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 operates invisibly, so that the mobile station subscriber is unable to detect it. The system does not interfere with the external mobile GSM networks.").

[52] *Active GSM Interceptor*, ABILITY, http://www.interceptors.com/intercept-solutions/ Active-GSM-Interceptor.html (last visited Aug. 13, 2013) ("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,

3. *Mass Surveillance of Network Activity*

Whereas "lawful intercept" technologies enabled under CALEA and in ETSI standards enable targeted interception of named individuals to respond specifically to "lawful" requests, there are now companies trading in technologies and services that enable large-scale interception, collection, and analysis of communications.[54] Despite significant growth in bandwidth, companies are developing and deploying technologies to intercept and collect data on high-speed streams at various points on communications networks, even under-sea fibre-optic cables.[55] This enables simultaneous interception of large populations[56] and interception of wide categories of information[57] for later analysis. Metadata and content gleaned from these interceptions can be analysed

---

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.").

[53] *Cell Phone Intercept Apparatus*, VIEW SYSTEMS, http://viewsystems.com/pdf/CIA_11_20_06.pdf (last visited Aug. 13, 2013) ("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.").

[54] *See* David A. Fulghum, *Electronic Blitz*, AVIATION WK. & SPACE TECH., Mar. 29, 2010, at 58.

[55] *Id.* (includes quotations from Glimmerglass, a provider of interception capabilities, from their director of business development, Keith May: "We believe our 3D MEMS technology—as used by governments and various agencies—is involved in the collection of intelligence from sensors, satellites and undersea fiber systems . . . We are deployed in several countries that are using it for lawful interception. They've passed laws, publicly known, that they will monitor all international traffic for interdiction of any kind of terrorist activity. With that they need to select the wavelengths they want to look at, demultiplex the signals and then selectively send them places for processing and monitoring.").

[56] Utimaco, a member of the Sophos Group, advertises the capability of monitoring virtually unlimited numbers of subscribers, with up to 100,000 simultaneous targets on telephony networks, and generate metadata at 100,000 records per second. UTIMACO, LIMS ACCESS POINTS: REALTIME NETWORK MONITORING FOR LAWFUL INTERCEPTION AND DATA RECOGNITION (2013), *available at* http://lims.utimaco.com/fileadmin/assets/brochures_datasheets_whitepapers/UTIMACO_AP_BROCHURE_EN.pdf; UTIMACO, DATA RETENTION SUITE: AUTOMATED DATA RETENTION FOR TELECOMMUNICATIONS SERVICE PROVIDERS (2013), *available at* http://lims.utimaco.com/fileadmin/assets/brochures_datasheets_whitepapers/UTIMACO_DRS_BROCHURE_EN.pdf.

[57] One company, Amesys, states in a presentation entitled "From Lawful to Massive Interception" that under massive surveillance you can "[a]nalyse all the communications of the link" and create an "[a]rchive of all Internet traffic—Smart search engine to recover communications in the past" and "[a]ll the communications are store[d] in the system." *From Lawful to Massive Interception: Aggregation of Sources*, AMESYS (2008), http://reflets.info/wp-content/uploads/2013/06/21_200810-ISS-PRG-AMESYS.pdf.

using speaker and language recognition,[58] mass location-tracking and more traditional methods of analysis including keyword and topic searching, and identifying networks of individuals and groups.[59]

From our research, these technologies are being deployed across the world, often without a clear legal framework governing their use. In fact, there are few cases where countries have explicitly passed laws regulating their use.

II. THE RISKS OF MODERN COMMUNICATIONS SURVEILLANCE

The technologies we identify beg the question of how our existing legal frameworks will integrate these new developments. Unfortunately, Parliaments and Congresses around the world have been slow to respond to such new technologies and the need for new safeguards. Most legislative activity has been on the expansion of surveillance powers. While there have been some developments in laws protecting the personal data of consumers and citizens, these are relatively silent on the use of surveillance technologies directly by law enforcement and intelligence agencies.[60]

This is not to say that there is a continual onslaught of surveillance law; in fact, in some countries proposed communications surveillance policies have failed to gain the traction necessary to become law.[61] This lack of new law means that old legal regimes continue to apply, which are often silent on these new techniques. Without new laws, there are limited means for establishing new safeguards. This problem may be systemic. As Stephen Smith notes, the

---

[58] Agnitio develops technologies for passive interception and speaker identification. *See About Agnitio*, AGNITIO, http://agnitio-corp.com/quienessomos.php (last visited Aug. 13, 2013).

[59] For instance, NiceTrack from NICE provides nationwide interception and analysis of communications metadata to expose and visualise target networks, identify suspicious patterns, and "handles mass volumes of subscriber data and delivers accurate, reliable target positioning in real time," and "enables unobtrusive monitoring so that targets are unaware of its presence and cannot prevent LEAs and intelligence organizations' tracking activities." *NiceTrack Location Tracking Center: Accurate Mobile Tracking Solutions for LEAs and Intelligence Organizations*, NICE SYSTEMS, http://www.nice.com/Intelligence-lea/location-tracking (last visited Aug. 21, 2013).

[60] For instance, see generally Council Directive 95/46, 1995 O.J. (L 281) 31 (EC) on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[61] In 2013 alone, proposed communications surveillance policies in Australia, Canada, and the United Kingdom have faced significant legislative opposition. *See* ACCESS TO COMMUNICATIONS DATA, *supra* note 37; PARLIAMENTARY JOINT COMM. ON INTELLIGENCE & SEC., PARLIAMENT OF THE COMMONWEALTH OF AUSTL., REPORT OF THE INQUIRY INTO POTENTIAL REFORMS OF AUSTRALIA'S NATIONAL SECURITY LEGISLATION, at viii (2013), *available at* http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/report.htm; Laura Payton, *Government Killing Online Surveillance Bill*, CBC NEWS (Feb. 11, 2013), http://www.cbc.ca/news/politics/story/2013/02/11/pol-rob-nicholson-criminal-code-changes.html (describing the withdrawal of proposed reforms to Canadian surveillance laws).

location tracking capabilities of cell phones came to Congress's attention in 1994, but as of today there have been no changes to the Electronic Communications Privacy Act clarifying the appropriate legal standard by which law enforcement agencies may obtain that location data.[62] Congress does not even have adequate information to ascertain the nature and extent of such surveillance because of inadequate reporting about its use.[63] David Gray and Danielle Citron note that both Democrat- and Republican-sponsored bills attempting to regulate surveillance died in committee in the 112th Congress.[64] As a result, governments that are using these techniques may be doing so without a clearly applicable legal framework.

Courts have not provided much more insight on how these technologies are to be used. "Until 2010, no appellate court had ever addressed the legal standard applicable to cell phone-tracking orders, even though magistrate judges were issuing tens of thousands of such orders every year without appellate guidance."[65] Orin Kerr argues that we can only count on courts to step in to regulate stable technologies.[66] Unlike automobiles and handguns, communications technologies are in flux. According to Kerr, generally the courts don't review a technology until long after it has been introduced—the technology must be used in the course of investigating a criminal offence, it must yield evidence of a crime, lead to an arrest, and then lead to a constitutional challenge.[67] This takes time. Though the telephone was invented in 1876, it wasn't until *Olmstead* in 1928 that the Supreme Court considered it.[68] Pen registers, that record the telephone numbers called from a line, were not considered until 1979.[69]

This appears to be changing. In Part III, we are able to identify some recent lower court cases in which the technologies described in Part II are being questioned. In the absence of statutory movement, judicial activity may be required because of the following inherent risks posed by these new technologies.

---

[62] *See* Stephen Wm. Smith, *Gagged, Sealed & Delivered: Reforming ECPA's Secret Docket*, 6 HARV. L. & POL'Y REV. 313, 316 (2012).

[63] *See id.*

[64] David Gray & Danielle Keats Citron, *A Shattered Looking Glass: The Pitfalls and Potential of the Mosaic Theory of Fourth Amendment Privacy*, 14 N.C. J.L. & TECH. 381, 392 n.41 (2013) (pointing to the Preserving Freedom from Unwarranted Surveillance Act of 2012, Protecting America's Privacy Act of 2012, and Location Privacy Protection Act of 2012).

[65] Smith, *supra* note 62, at 326.

[66] Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 805 (2004).

[67] *See id.* at 868.

[68] *See id.* at 869 n.404.

[69] *See id.* at 869.

A. *Secrecy*

Unlike traditional search and seizure, these forms of surveillance are by nature secretive. The implementations of most offensive technologies, mobile monitoring devices, and mass communications surveillance are designed to ensure that the individual is unaware of their use.

The secrecy of surveillance is already problematic under regulated regimes. For instance, Smith notes that under ECPA there is a regime of indefinite sealing, nondisclosure, and delayed-notice provisions that results in ECPA surveillance orders being concealed from unsuspecting targets, the general public, and even other arms of government.[70]

This reinforces why notice requirements in the Wiretap Act and Stored Communications Act are important privacy protections that particularly benefit those who are subjects of surveillance but never charged with a crime.[71] While it is possible to notify an individual that his or her device was penetrated using an offensive technology, it is more challenging to notify every mobile phone user, or everyone who used a trans-Atlantic cable, that his or her communications were intercepted, or metadata-collected and stored for later analysis. Recent events demonstrate the reluctance of at least the U.S. and UK Governments to make such mass surveillance public. The United States kept secret for years the now infamous Verizon order, which required the mass disclosure of communications metadata.[72] The likelihood of the public being notified that fiber-optic cables are being monitored directly by governments is equally small, as was again demonstrated by the leaks regarding the UK's ongoing Tempora program that allegedly taps into those very cables.[73] Accordingly, courts need to step in to assess, in the first instance, whether these technologies should even be deployed, and thereafter when and if notification of targets is appropriate.

B. *Directed Surveillance: The Two-Body Problem*

The secret use of these technologies is further enabled by the way they work; they do not necessarily require the participation of third-party service providers.[74] Each of the techniques identified above can be applied directly against their targets. Offensive technologies can be uploaded onto the target device, over the Internet, without seeking approval from a third party. IMSI catchers and mobile interception devices make it possible for the government directly to monitor mobile communications without having to involve the

---

[70] *See* Smith, *supra* note 62, at 314.

[71] *See* Pell & Soghoian, *supra* note 33, at 186.

[72] *See* Greenwald, *supra* note 25.

[73] *See* MacAskill et al., *supra* note 26.

[74] This new development runs counter to the current trend in communications surveillance scholarship to focus on the role of the third-party service providers in government surveillance.

carriers. Mass surveillance technologies directly tap into data streams, once physical access to the stream has been obtained. This physical access still may require some cooperation from third parties. But while the law governing that access is unclear, there is some evidence that these arrangements are well established.[75] Once access is negotiated, it is possible for governments to use the mass surveillance technologies to obtain communications data without having to involve the companies themselves.

As a result of this directed surveillance, there is less of a push for regulatory and statutory guidance on how the surveillance is conducted. The third-party service providers, which have pushed for such guidance, either to protect their users or to immunize themselves from liability, have been removed from the equation.[76] In many cases the targets may not even know that they have been under scrutiny. It is thus possible that these techniques are being secretly deployed without any regulatory guidance at all. Requiring court approval before these technologies are used, therefore, may be one of the few ways to assess whether their deployment is consistent with privacy and other legal concerns.

C. *Overbreadth*

These techniques also raise scoping problems. A mobile monitoring device, though geographically limited, will nonetheless collect data on all nearby mobile phones and devices that connect to it, including those that are unrelated to a given investigation. Similarly, mass surveillance technologies collect information on all communications going through a single fiber, cable, and/or network.[77] With these technologies, the act of interception is no longer targeted

---

[75] For an emerging collection of agreements between the U.S. Government and telecommunications companies around the world, see PUB. INTELLIGENCE, *supra* note 18, which includes agreements between international providers and various agencies of the U.S. Government. According to Craig Timberg & Ellen Nakashima, *Agreements with Private Companies Protect U.S. Access to Cables' Data for Surveillance*, WASH. POST, July 6, 2013, http://articles.washingtonpost.com/2013-07-06/business/40406049_1_u-s-access-global-crossing-surveillance-requests, the agreements require companies to maintain what amounts "to an internal corporate cell of American citizens with government clearances" ensuring that "when U.S. government agencies seek access to the massive amounts of data flowing through their networks, the companies have systems in place to provide it securely."

[76] *See, e.g.*, Brandon Bailey, *Exclusive: Yahoo Seeks To Reveal Its Fight Against NSA Prism Requests*, SAN JOSE MERCURY NEWS (July 11, 2013), http://www.mercurynews.com/business/ci_23635466/yahoo-asks-secret-surveillance-court-unseal-files (describing Yahoo's recent court battle to reveal its previous efforts to challenge U.S. Government requests for user information under FISA); Karl Bode, *FISA: AT&T, Verizon Lobbyists Win Again*, DSLREPORTS.COM (July 10, 2008), http://www.dslreports.com/shownews/FISA-ATT-Verizon-Lobbyists-Win-Again-95994 (noting AT&T, Verizon, and Sprint spent millions of dollars lobbying for an immunity provision to be added to FISA, protecting them from their previous acquiescence with government requests for user data).

[77] The amount of data encountered with mass surveillance necessarily needs some form of "filtering" because our abilities to monitor, for instance, a 100 GB/s medium would

at an individual, but rather uses over-collection and analysis to identify specific targets.

This breadth of application also raises issues of jurisdiction. For instance, the use of offensive techniques may involve infecting devices in unknown jurisdictions; the government targeting a device may not know where the device is located when the offensive technology is deployed. This links back to the policies mentioned above that are currently being considered by the Dutch Government and within the Council of Europe that seek to authorize remote searching of computers in other jurisdictions.[78]

Mass surveillance techniques certainly collide on jurisdiction and breadth. In his analysis of interim updates to FISA, Orin Kerr accepts that surveillance now "tends to be divorced from the identity and location of the parties to the communication."[79] Instead, governmental authorities end up searching for traffic characteristics rather than known identities.[80]

In sum, we are inviting techniques that involve the application of surveillance against unknown entities. These techniques will not only be used to identify a given suspect, but they can be used to speculate on who should be targeted by utilizing mass surveillance, such as by identifying all mobile phones in an area believed to contain criminal suspects or the trawling through an undersea fibre-optic cable to draw out the identities of individuals communicating in a specific language and/or using a particular set of words. As recent disclosures have uncovered, we are in the process of redefining key terms in our legal safeguards, including "relevant"[81] and even "collection."[82] Such significant changes in the scope of surveillance need to be thoroughly vetted.

---

require vast amounts of storage, or analysis at the rate of 100 GB/s, both of which are very difficult to resource. *See, e.g.*, Glenn Greenwald, *XKeyscore: NSA Tool Collects "Nearly Everything a User Does on the Internet,"* GUARDIAN, July 31, 2013 [hereinafter *XKeyscore Program*], http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data (describing how the collection of vast amounts of information is filtered down for analysis). As such, the mass monitoring techniques are able to conduct triage by analyzing and segmenting traffic, which also requires the monitoring of the communications—quite differently from ignoring all the calls going into a telephone company and only focusing on the ones being channeled to a specific suspect. *Compare* Smith v. Maryland, 442 U.S. 735, 745–46 (1979) (applying a pen register to monitor the calls of a single individual), *with XKeyscore Program*, *supra* (alleging NSA collects all data then runs searches for information it deems relevant). These techniques include the ability to identify languages being spoken, individual speakers, keywords, topics of conversations—all of which means that much broader categories are "intercepted" in the process of deciding which deserve further scrutiny. *See, e.g.*, *id.* As a result we are redefining "interception" as it becomes a mass surveillance activity for the purpose of weeding out specific data.

[78] *See supra* notes 41–42.

[79] *See* Orin S. Kerr, *Updating the Foreign Intelligence Surveillance Act*, 75 U. CHI. L. REV. 225, 234 (2008).

[80] *See id.*

[81] *See* Lichtblau, *supra* note 12, at A1; Jennifer Valentino-Devries & Siobhan Gorman, *Secret Court's Redefinition of "Relevant" Empowered Vast NSA Data-Gathering*, WALL ST.

D. *Applicability of Constitutional Protections Against Unreasonable Search and Seizure*

It is by no means clear how constitutional protections may apply to the new technologies. In Part III, we contend that these technologies raise important Fourth Amendment concerns. But not all commentators are as convinced. For instance, some, such as Orin Kerr, focus on a property rights approach to the Fourth Amendment,[83] with its strong focus on exclusion. The police can look into windows, do aerial searches, use informants—all actions that arguably violate privacy but don't violate property rights. Under this approach, remotely accessing a computer might not be a protected invasion if it is not considered a trespass. It is also not immediately clear if the copying of content from devices constitutes a seizure.[84]

In contrast, as we will discuss in more detail below, Susan Brenner rejects the property-based approach to the Fourth Amendment, and concludes that the use of an offensive technology to access a computer is "functionally analogous to the one Katz found himself in," as described in the U.S. Supreme Court's groundbreaking decision.[85] Both the computer user who is connected to a network and Katz were using a method of communication that is reliant upon technology with the reasonable assumption that the content of their communication is private.[86] Brenner also contends that copying data is a seizure, even though the user retains a copy.[87] Instead, she argues that the very loss of exclusive possession by the individual who owns the device and the data is the meaningful interference with the possession of the property.[88] The contrasting approaches of commentators like Kerr and Brenner demonstrate that the applicability of the Fourth Amendment to new technologies is far from settled.

Further challenges arise when we consider the use of mobile monitoring devices and mass surveillance systems because of the type of information they collect. Both of these techniques may collect communications metadata in bulk, sometimes deriving it from intercepted content. Citing *Smith v. Maryland* and

---

J., July 8, 2013, http://online.wsj.com/article/SB10001424127887323873904578571893758853344.html.

[82] *See The Government's Word Games When Talking About NSA Domestic Spying*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/nsa-spying/wordgames (last visited Aug. 14, 2013).

[83] *See* Kerr, *supra* note 66, at 813. He notes: "So long as the surveillance does not invade the individual's right to exclude others—the very essence of the property right—the surveillance generally does not violate his reasonable expectation of privacy." *Id.*

[84] *See id.* at 814.

[85] Susan W. Brenner, *Fourth Amendment Future: Remote Computer Searches and the Use of Virtual Force*, 81 MISS. L.J. 1229, 1243 (2012).

[86] *Id.*

[87] *See id.* at 1245.

[88] *Id.*

the third party doctrine (which generally holds that a person cannot retain a reasonable expectation of privacy in information given to a third party), Orin Kerr has raised questions as to whether such metadata is subject to constitutional protections.[89] But because of these new technologies' broad collection capabilities, the bulk "metadata" collected, especially when it is generated from content, is not the same as metadata that is "given" to third parties for processing. For instance, a technique exists to identify the language of a communication from its content. Some may be quick to reduce the identification of the language used to the lower status of "metadata," but it first requires the invasive act of intercepting content. Such surveillance activity was not foreseen by the Court in *Smith v. Maryland.*

E. *Other Constitutional Concerns*

A final area of contention with these techniques is that they may conflict with other constitutionally protected activities.

In the case of mobile and mass surveillance techniques, the purpose of collection may be for the identification of groups and individual affiliations. An IMSI catcher could identify all individuals attending a public protest. Mass surveillance may be intended to reveal all members of a particular political organization. Both uses are likely to chill freedom of expression and association. To date this issue mostly has been missed: pointing to the *ACLU v. NSA*,[90] *Al-Haramain v. Bush*,[91] and *Clapper v. Amnesty*[92] courts, Neil Richards contends that, in addressing surveillance, courts ignore First Amendment concerns.[93] We attempt to address this omission by taking such concerns into account in the following analysis.

III. HOW SHOULD COURTS APPROACH THESE NEW TECHNIQUES?

The above considerations lead us to the concrete question of how use of these emerging surveillance technologies should be treated by U.S. courts. Whether the courts or the legislature are the better forum to address such use is an open question—but the fact remains that the lower courts, whatever their competencies, are already being forced to tackle the constitutionality of offensive technologies, mobile surveillance, and mass surveillance.

For example, the Southern District of Texas recently considered a request for a warrant authorizing the use of an offensive technology the court described

---

[89] *See* Kerr, *supra* note 15, at 596–97.

[90] ACLU v. NSA, 493 F.3d 644, 657 (6th Cir. 2007).

[91] Al-Haramain Islamic Found., Inc. v. Bush, 507 F.3d 1190, 1201–05 (9th Cir. 2007).

[92] Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1150–53 (2013).

[93] Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1951 (2013).

as "data extraction software."[94] According to the court, the software would have allowed the government to "search the [target] computer's hard drive, random access memory, and other storage media; to activate the computer's built-in camera; to generate latitude and longitude coordinates for the computer's location; and to transmit the extracted data to FBI agents."[95] But, the government did not know whom it would be targeting with the software—indeed, part of the purpose of the software was to help the government identify their suspect. The agents intended to install the software on an unknown "target" computer by sending it to an email address that was implicated in a bank fraud investigation.

The court questioned the warrant application, raising several issues that highlight problems that may arise with the use of offensive technologies. First, the government did not, and seemingly could not, provide assurances that an innocent computer or person would not become the target of surveillance.[96] By sending the data extraction software via email, the government might inadvertently infect any number of computers if that email was opened, for instance, on a library computer, or in an Internet café, or on any computer that did not belong to the perpetrator.[97] Second, the government failed to explain how it would limit the collection of data to only that which would be relevant to the investigation. The court reasoned the broad capabilities of the data extraction software could not be "fairly described as capturing 'only limited amounts of data,'" and was especially concerned that innocent people might be captured on the computer's camera.[98] Third, it was not clear to the court that the government could not obtain the information it sought through less intrusive means, such as by seeking the identity of the person who owned the email address from the email service provider via the procedures outlined in the Stored Communications Act.[99] Based on these concerns, among others, the court refused to issue the warrant.

Two other courts were recently called upon to consider the use of mobile monitoring devices—in these cases the surveillance technique involved the more restrained application of the technique of impersonating a mobile base station in order to gain access to device identifiers, i.e. IMSI catchers.[100] The

---

[94] *In re* Warrant To Search a Target Computer at Premises Unknown, No. H-13-234M, 2013 WL 1729765, at *1 (S.D. Tex. Apr. 22, 2013).

[95] *Id.*

[96] *Id.* at *4.

[97] *Id.*

[98] *Id.* at *6.

[99] *Id.* at *5.

[100] The name of the devices used in these cases was "Stingray." Our understanding is that the use of these devices in these two cases was limited to capturing the metadata, and not impersonating a base station to intercept communications content. For a helpful summary, see Hanni Fakhoury & Trevor Timm, *Stingrays: The Biggest Technological Threat to Cell Phone Privacy You Don't Know About*, ELECTRONIC FRONTIER FOUND. (Oct. 22, 2012), https://www.eff.org/deeplinks/2012/10/stingrays-biggest-unknown-technological-threat-cell-phone-privacy.

Southern District of Texas again heard the first of the two cases, in which the Drug Enforcement Agency (DEA) wanted to use an IMSI catcher to determine the cell phone number of a suspected drug dealer.[101] The government sought authorization for the IMSI catcher under the more lenient statutory standard established for use of pen registers and trap and trace devices.[102] In its attempt to analogize an IMSI catcher to a pen register, the government was vague in its description of how the device would function, especially with regard to how the cellphone numbers and other information the stingray would inevitably capture from innocent cell phone users would be treated.[103] The presiding magistrate judge ultimately concluded an IMSI catcher is not analogous to a pen register because, among other things, a pen register "seek[s] information about a particular telephone [number]," while the purpose of the IMSI catcher was to allow the DEA to determine the phone number of the suspect they were tracking.[104] Accordingly, if the government wanted to use an IMSI catcher, it would need to seek a warrant, satisfying normal Fourth Amendment standards.[105]

Shortly thereafter, the District of Arizona had the opportunity to consider whether such a warrant could authorize the use of an IMSI catcher to assist in locating an individual.[106] In *United States v. Rigmaiden*, the court previously had issued a warrant allowing the government to use the device to identify the location of an aircard[107] allegedly being used by the defendant to file fraudulent tax returns.[108] At trial, the defendant and the American Civil Liberties Union, as amicus, challenged the sufficiency of that warrant.[109] Of particular concern was the lack of detail provided to the court regarding the capabilities of the mobile tracking device, specifically its ability to capture innocent third-party cellphone and aircard information.[110] The court found that the omission of this detail did not invalidate the warrant, although its impact appears to have been blunted by hindsight. As the court noted, the government stayed within the scope of the warrant it sought:

---

[101] *In re* The Application of the United States for an Order Authorizing the Installation and Use of a Pen Register and Trap and Trace Device, 890 F. Supp. 2d 747, 748 (S.D. Tex. 2012).

[102] *Id.* at 748–51.

[103] *Id.* at 749.

[104] *Id.* at 750–51.

[105] *Id.* at 752.

[106] United States v. Rigmaiden, No. CR08-814-PHX-DGC, 2013 WL 1932800 (D. Ariz. May 8, 2013).

[107] An aircard, as explained by the court, is a broadband access card, generally provided by a cellular telephone company, that can be "used to make a wireless connection between a computer and the Internet." *Id.* at *1.

[108] *Id.*

[109] *Id.* at *14–22.

[110] *Id.* at *19–22.

> [T]he agents in this case did not seek to capture third-party cell phone and aircard information so they could use it in a criminal investigation, nor is there any evidence that they used the third-party information in that manner. To the contrary, the evidence presented by the government and Defendant shows that third-party information was deleted from the mobile tracking device immediately after the aircard was located.[111]

All three of these cases highlight some of the concerns we have already raised regarding the emerging technologies we are here discussing—their ability to capture far more information than was previously available to law enforcement, including significant details about innocent individuals who are in no way implicated in the investigation. This concern is brought to the fore by mass surveillance technologies. The vast majority of information caught by such means will be irrelevant to any criminal or national security investigation. Recent news reports revealed the U.S. Government is engaging in just such mass surveillance.[112] Challenges to certain of those practices are beginning to reach the courts.[113]

As the cases addressing offensive technologies and mobile monitoring devices demonstrate, courts are struggling with how to fit these new technologies into the Fourth Amendment framework. The following is our attempt to provide some guidance on that issue. We conclude that, under current Supreme Court doctrine,[114] all of these new technologies raise significant Fourth Amendment concerns. Given the rapid evolution of such surveillance

---

[111] *Id.* at *20.

[112] In June 2013, the *Washington Post* and the British newspaper the *Guardian*, published a series of leaked slides describing U.S. Government surveillance activities. *See PRISM Data-Collection*, *supra* note 26; Glenn Greenwald & Ewen MacAskill, *NSA Prism Program Taps in to User Data of Apple, Google and Others*, GUARDIAN, Jun. 6, 2013, http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data. One of the slides describes the government's ability to collect "communications of fiber cables and infrastructure as data flows past." *PRISM Data-Collection*, *supra* note 26. This is the very sort of collection to which mass surveillance technologies could be applied. The FBI and NSA are already collecting data from service providers en masse, as evidenced by another recently leaked order requiring Verizon to provide the agencies with call detail records for *all* of its U.S. users. *See Verizon Forced To Hand over Telephone Data—Full Court Ruling*, GUARDIAN, June 5, 2013, http://www.guardian.co.uk/world/interactive/2013/jun/06/verizon-telephone-data-court-order.

[113] *See, e.g.*, ACLU's Memorandum of Law in Support of Plaintiffs' Motion for a Preliminary Injunction at 21–23, ACLU v. Clapper, No. 13-cv-03994-WHP (S.D.N.Y. Aug. 26, 2013), ECF No. 26, *available at* https://www.aclu.org/files/pdfs/natsec/clapper/2013.08.26%20ACLU%20PI%20Brief.pdf.

[114] We work within current Supreme Court doctrine, despite the many valid criticisms that have lodged against the current regime, because these cases are the ones the lower courts, which are currently struggling with these new technologies, are bound to follow. We also see, in concurrences in *United States v. Jones*, some movement toward a more holistic conception of the Fourth Amendment that lower courts may draw on as they tackle these difficult issues. *See* United States v. Jones, 132 S. Ct. 945, 954–57 (2012) (Sotomayor, J., concurring); *id.* at 957–64 (Alito, J., concurring).

techniques, and the privacy interests they implicate, the function of a court to balance the needs of law enforcement against those interests becomes essential.

* * *

The Fourth Amendment prohibits "unreasonable searches and seizures."[115] We begin our analysis with the question of whether the use of each of our enumerated technologies constitutes a search under the Fourth Amendment—the first step in determining whether the considered activity is subject to that Amendment's reasonableness requirement. Since *Katz*, to determine whether a given activity constitutes a search, the Supreme Court most frequently asks whether the affected individual had a reasonable expectation of privacy in the object of the search.[116] A search occurs if "the individual manifested a subjective expectation of privacy in the object of the challenged search" and "society [is] willing to recognize that expectation as reasonable."[117] More recently, the Court has revived another conception of what constitutes a search, holding that a physical occupation of private property for the purpose of obtaining information also falls within the realm of activities proscribed by the Fourth Amendment.[118] We find the reasonable expectation of privacy standard more applicable to the remote-access technologies we here consider, and thus proceed with our analysis on that basis.[119]

A. *Offensive Technologies*

With regard to offensive technologies, Professor Susan Brenner has already made a persuasive argument that their use, at least on a computer located in a person's home or office, constitutes a search.[120] Professor Brenner follows the lead of several lower courts in analogizing a computer to a closed container, the accessing of which is considered a search.[121] She further reasons that connecting a computer to the Internet does not vitiate a person's reasonable expectation of privacy in its contents. Like the phone booth in *Katz*, while the computer may provide its user with a connection to the outside world, in each case there is evidence that the user expects her content to remain private; "the

---

[115] U.S. CONST. amend. IV.

[116] *See, e.g.*, California v. Ciraolo, 476 U.S. 207, 211 (1986).

[117] *Id.*

[118] *Jones*, 132 S. Ct. at 949.

[119] Orin Kerr contends that the "reasonable expectation of privacy" test from *Katz* is "more of a revolution on paper than in practice" in that courts seem to focus more on the interference with property rights. Kerr, *supra* note 66, at 807. "The result is a critical gap between privacy rules the modern Fourth Amendment provides and privacy rules needed to effectively regulate government use of developing technologies." *Id.*

[120] Brenner, *supra* note 85, at 1239.

[121] *Id.*

computer user because she is on her computer in her home or office, and Katz because he was in a phone booth the door of which was securely closed."[122]

We would take Brenner's argument further. Brenner confines herself to analogizing a computer to a container. But a modern computer is unlike any other container. It can store vast amounts of information about every aspect of a person's life, including: financial information, medical records, private correspondence, diaries recording private thoughts, work product, photographs, home videos, books, music, records of purchases, and much more. A computer's massive storage capacity may even encourage the accumulation of far more data than would previously have been maintained in a person's house or personal papers.[123] And computers are not merely passive receptacles. Modern computers often incorporate cameras and microphones that, under the control of an offensive technology, could record even more information about the computer's surroundings, from private conversations to pictures and video of the objects and persons who happen to be in front of the camera. Essentially, computers have become repositories of and portals into the most intimate aspects of our lives. To access a computer is thus the equivalent of invading a person's home in the amount and quality of information such access can provide.

The Supreme Court has repeatedly recognized that the home receives the highest level of protection. Almost any intrusion into that sacred space will constitute a search. As the Court explained in *Silverman v. United States*: "The Fourth Amendment, and the personal rights which it secures, have a long history. At the very core stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion."[124] It is not much of a conceptual leap to consider modern computers in the same way and grant them the same level of protection, especially from offensive technologies that are capable of opening a window into the most intimate aspects of a person's life.

This conclusion is bolstered when we assess where a computer is likely to fall in the spectrum of spaces in which the Court has held a person has a reasonable expectation of privacy. At the top of that spectrum, right next to the home, is a rented hotel room. According to the Court, "[n]o less than a tenant of

---

[122] *Id.* at 1243.

[123] *See* Paul Ohm, *Massive Hard Drives, General Warrants, and the Power of Magistrate Judges*, 97 VA. L. REV. IN BRIEF 1, 6–8 (2011), http://www.virginialawreview.org/sites/virginialawreview.org/files/ohm.pdf (describing in detail the incredible storage capacity and varied content stored on modern computers).

[124] Silverman v. United States, 365 U.S. 505, 511 (1961) (citation omitted); *see also* Kyllo v. United States, 533 U.S. 27, 37 (2001) ("In the home, our cases show, *all* details are intimate details, because the entire area is held safe from prying government eyes."); United States v. Karo, 468 U.S. 705, 714 (1984) ("At the risk of belaboring the obvious, private residences are places in which the individual normally expects privacy free of governmental intrusion not authorized by a warrant, and that expectation is plainly one that society is prepared to recognize as justifiable. Our cases have not deviated from this basic Fourth Amendment principle.").

a house, or the occupant of a room in a boarding house . . . a guest in a hotel room is entitled to constitutional protection against unreasonable searches and seizures."[125] A hotel room is unlikely to contain as much private information as a computer, however. At most, unless it is a long-term rental, such a space will hold a snapshot of a person's life—luggage, immediately needed sundries, the person herself. A computer can document much more, potentially years' worth of intimate details and communications. The virtual wall a computer erects around our personal information is as essential to our understandings of a personal space as the physical walls of a hotel room.

The Court has also seen fit to protect personal luggage from unreasonable search.[126] Much like the locked footlocker at issue in *Chadwick*, a computer's contents "are not open to public view," are not "subject to regular inspections and official scrutiny on a continuing basis," and the computer is "intended as a repository of personal effects."[127] All together, these characteristics evidence a substantial expectation of privacy in the contents of a computer.

This expectation attaches despite the fact that the proliferation of high capacity "smart" phones and laptops means that many computers can now travel with a person from inside the home, to the office,[128] to anywhere else she may go. Personal luggage is similarly mobile, yet has been accorded an expectation of privacy.[129] Furthermore, even if we were to assume the contents of a mobile computer, in and of themselves, are not subject to such an expectation, that computer is almost certain to be located within a person's home or office for a significant amount of time each day. Most of us are quite familiar with the rituals of charging our cellular phones on our nightstands each night, or carting our laptops between home and office. If, while the computer resides in such a protected place, the government could not gain access to it without a warrant,[130]

---

[125] Stoner v. California, 376 U.S. 483, 490 (1964).

[126] *See, e.g.*, United States v. Chadwick, 433 U.S. 1, 11 (1977) ("By placing personal effects inside a double-locked footlocker, respondents manifested an expectation that the contents would remain free from public examination. No less than one who locks the doors of his home against intruders, one who safeguards his personal possessions in this manner is due the protection of the Fourth Amendment Warrant Clause."); *see also* Bond v. United States, 529 U.S. 334, 339 (2000) (holding an officer unreasonably searched a bag by merely squeezing it to determine if it contained contraband).

[127] *Chadwick*, 433 U.S. at 13.

[128] The office, like the home, is subject to a heightened level of privacy protection under which a governmental search, in most circumstances, will be unreasonable without a warrant. *See, e.g.*, O'Connor v. Ortega, 480 U.S. 709, 716 (1987); Mancusi v. DeForte, 392 U.S. 364, 364 (1968).

[129] *Chadwick*, 433 U.S. at 13.

[130] As the Court so clearly stated in *Kyllo v. United States*, no matter what expectation of privacy might normally attach to the subject of a search, "[i]n our home, our cases show, *all* details are intimate details, because the entire area is held safe from prying government eyes." Kyllo v. United States, 533 U.S. 27, 37 (2001). Accordingly, the Court refused to allow the government to use a new technology to reach into that protected space, even though the technology made doing so possible without crossing the threshold of the home. *Id.* at 40 ("Where, as here, the Government uses a device that is not in general public use, to

then the government should not be able to install an offensive technology on that device merely because, for some fractional amount of time, it may be located outside of the protected sphere. This is especially true given the ability of offensive technologies to not only access the computer or phone, but to also convert it into a video and audio bug with which to invade the home or office—something that, pursuant to the Wiretap Act, cannot occur without a warrant.[131]

Accordingly, like in a home, a hotel room, a closed container, or personal luggage, a person has a reasonable expectation of privacy in the contents of her computer, and in its ability to transmit audio, video, or locational information regarding her surroundings when those surroundings are likely to constitute traditionally protected areas such as the home and the office. In order to use offensive technologies to search a computer, therefore, the government must obtain a warrant, unless one of the very limited exceptions to the warrant requirement applies.[132]

Brenner again astutely concludes that most of these exceptions are unlikely to attach to the use of offensive technologies.[133] When dealing with phone tapping, another form of electronic surveillance, the Supreme Court came to the similar conclusion in *Katz*:

> It is difficult to imagine how any of those exceptions could ever apply to the sort of search and seizure involved in this case. Even electronic surveillance substantially contemporaneous with an individual's arrest could hardly be deemed an "incident" of that arrest. Nor could the use of the electronic surveillance without prior authorization be justified on grounds of "hot pursuit." And, of course, the very nature of electronic surveillance precludes its use pursuant to the suspect's consent.[134]

In most circumstances, therefore, in order to deploy offensive technologies, the government must obtain a warrant. Pursuant to the Fourth Amendment, "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[135] As we noted, *supra*, this particularity requirement may not always be easy to satisfy when deploying an offensive technology. Following the lead of the Southern District of Texas, courts should press anyone requesting authorization to deploy an offensive technology for assurances that probable cause exists that a *particular* computer or phone

---

explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant.").

[131] *See* Wiretap Act, 18 U.S.C. §§ 2510–2522 (2012).

[132] *See* United States v. Jeffers, 342 U.S. 48, 51 (1951) ("Only where incident to a valid arrest, or in 'exceptional circumstances,' may an exemption [to the warrant requirement] lie." (citations omitted)).

[133] Brenner, *supra* note 85, at 1251.

[134] Katz v. United States, 389 U.S. 347, 357–58 (1967).

[135] U.S. CONST. amend. IV.

contains the sought after evidence. If government officials cannot identify the computer they plan to infect—as they couldn't in the Texas case because all they had was an email address, not identifying information for a particular device—then they should not be allowed to proceed with the deployment of such intrusive technologies. Furthermore, given that a computer or a smartphone can store as much information as a home, a warrant should not authorize uninhibited access. Those seeking to use offensive technologies should be forced to specify exactly what "persons or things" they intend to seize, and to implement realistic and detailed minimization procedures to assure the warrant does not turn into a carte blanche to delve into every aspect of the subject's life.[136]

B. *Mobile Monitoring Devices*

We next look at the mobile phone surveillance technology commonly called "IMSI catchers." As we noted above, these devices can serve a variety of surveillance functions. The most basic use is to allow the identification of all mobile phones within range of the device by impersonating a mobile base station. Through the use of multiple devices, and triangulation, the IMSI catchers can also pinpoint the location of every mobile device within range—as occurred in *Rigmaiden*. At its most pernicious, the device can directly intercept content being transmitted by the mobile phone. When the government engages in any of these activities, a variety of privacy expectations are implicated.

We address each function of the IMSI catcher in reverse order, beginning with its ability to intercept content. We think there is little question that, pursuant to the Wiretap Act, if the government wants to intercept content with these devices it needs to obtain a warrant.[137] We do not delve further into that conclusion here because, as the two cases we summarize above demonstrate, IMSI catchers are more often being deployed for their two other functions: to locate or identify mobile phones within range of the device.

We next consider, therefore, the ability of IMSI catchers to locate a mobile phone. In their location tracking capabilities, IMSI catchers are analogous to the beeper the Supreme Court considered in *Karo*. That beeper was placed in a container of chemicals before that container was delivered to Karo, who was suspected of dealing drugs.[138] Using the beeper, agents were able to track the container as it moved from location to location, in the same way that IMSI catchers would allow the tracking of a mobile phone.[139] Several times the beeper revealed the container was located in private spaces into which the officers would not normally be able to enter without a warrant, including

---

[136] *See* Ohm, *supra* note 123, at 4 (cogently explaining the importance of placing such limitations on computer search warrants).

[137] *See* Wiretap Act, 18 U.S.C. §§ 2510–2522 (2012).

[138] *See* United States v. Karo, 468 U.S. 705, 708 (1984).

[139] *Id.*

homes.[140] As the government admitted to the Court, it would be almost impossible to determine, prior to using a tracking device—whether it be a beeper or an IMSI catcher—whether it might result in the tracking of a target object into a protected space like a home or office.[141]

This is illustrated by comparing the facts of *Karo* to its sister case *United States v. Knotts*.[142] In *Knotts*, the police similarly deployed a beeper to track a drum of drug-making material.[143] The Court held a warrant was not required for this tracking in large part because that drum fortuitously never entered a protected space.[144] Instead, the beeper in *Knotts* only revealed the drum's location on public roads or outside of the defendant's cabin.[145] A year later, in *Karo*, the Court faced an almost identical scenario, except that this time it happened that the container that held the beeper was transported into a home.[146] In these circumstances, the Court found the tracking of the beeper to be an unreasonable search because the officers were able to use the beeper to determine the location of the drum *within* the suspect's home.[147] The Court was unwilling to give the government free rein to use an electronic device to determine "whether a particular article—or a person, for that matter, is in an individual's home at a particular time."[148] As the government aptly pointed out in *Karo*, this holding, for all practical purposes, would force them to "obtain warrants in every case in which they seek to use a beeper, because they have no way of knowing in advance whether the beeper will be transmitting its signals from inside private premises."[149] An IMSI catcher similarly has the ability to determine "whether a particular article [a mobile phone]—or a person . . . is in an individual's home at a particular time."[150] The Court has repeatedly held such an electronic invasion, "to explore details of the home that would previously have been unknowable without physical intrusion," is a search that requires a warrant.[151]

For that reason, we contend a warrant should always be obtained prior to the use of an IMSI catcher given the possibility that its use will lead to an intrusion into a protected space, most especially a home, but also an office, a hotel room, and the myriad of other spaces the Court has acknowledged give rise to a reasonable expectation of privacy. Given that most people keep their mobile phones with them at all times, it seems probable that any person tracked,

---

[140] *Id.* at 708–10.
[141] *See id.* at 718.
[142] United States v. Knotts, 460 U.S. 276 (1983).
[143] *Id.* at 281–82.
[144] *Id.*
[145] *Id.* at 282.
[146] *Karo*, 468 U.S. at 708–10.
[147] *Id.* at 715.
[148] *Id.* at 716.
[149] *Id.* at 718.
[150] *Id.* at 716.
[151] Kyllo v. United States, 533 U.S. 27, 40 (2001); *see also Karo*, 468 U.S. at 718.

even for a relatively short period of time, is likely to enter one of these protected spaces. It is possible that an IMSI catcher could be deployed away from a target's protected space, but unless the device is in the middle of an uninhabited forest, desert, or at sea, it is likely to (over)collect the identifying information from other people's devices, and these individuals may very well be in protected spaces.

In the case of the use of IMSI catchers for long-term location tracking, our conclusion is bolstered by the sentiments expressed by the concurrences in *United States v. Jones*, the Court's most recent statement on location tracking.[152] While the majority opinion in *Jones* relied on a trespass theory to conclude the attachment of a GPS device to the defendant's vehicle was a search, Justices Sotomayor and Alito, in their concurring opinions, both reason that sustained location tracking could implicate Fourth Amendment concerns.[153] As Justice Alito so eloquently states, "society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period."[154] That statement applies with equal force to the movements of individuals, which can often be tracked by tracking their mobile phones. Justice Sotomayor similarly questions "whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on."[155] To the extent the use of IMSI catchers for long-term location tracking intrudes on these expectations of privacy, they provide further incentive for requiring the government to obtain a warrant before such use.

Similar concerns motivate our consideration of the IMSI catcher's ability to identify any mobile device in range by capturing its International Mobile Subscriber Identity ("IMSI"),[156] a unique number that identifies each mobile phone as it connects to a mobile network. The government may be able to use this capability in a variety of ways, ranging from identifying the IMSI of a specific mobile device, to cataloguing the identity of every mobile phone within range of the IMSI catcher. We suspect the latter has already occurred at large

---

[152] United States v. Jones, 132 S. Ct. 945 (2012).

[153] *Id.* at 954–57 (Sotomayor, J., concurring); *id.* at 957–64 (Alito, J., concurring).

[154] *Id.* at 964 (Alito, J., concurring).

[155] *Id.* at 956 (Sotomayor, J., concurring).

[156] We focus on the question of whether the capture of IMSIs implicates a reasonable expectation of privacy. We are well aware of the rigorous debate currently underway regarding whether a person has a reasonable expectation of privacy in her metadata more generally. See for instance, Kerr, *supra* note 15, which provides a review of the literature. While we think that there is a strong case for revisiting the so-called third-party doctrine, and tend to agree with those who argue modern metadata is analogous to content, a detailed discussion of that point is beyond the scope of this Article. We have written elsewhere on this. *See* Escudero-Pascual & Hosein, *supra* note 30, at 77–82; *International Principles on the Application of Human Rights to Communications Surveillance*, NECESSARY & PROPORTIONATE (July 10, 2013), https://en.necessaryandproportionate.org/text.

public gatherings. This ability to identify secretly and accurately every member of a crowd, via their phone's identifier, goes beyond what government authorities traditionally have been able to accomplish.[157] With normal visual surveillance, an officer might be able to identify a few members of a rally with which he was already familiar, but to identify every single person within range seems to be beyond normal human observational abilities. As such, much like the unprecedented secret monitoring of movements of concern to Justices Alito and Sotomayor, this ability of IMSI catchers implicates new privacy concerns.

Under the auspices of protecting freedom of expression and association, the Court has long held that an organization cannot be compelled by the government to identify its members.[158] People are also guaranteed the right to express themselves anonymously.[159] Both of these holdings set a reasonable expectation that a person, if he so chooses, can shield his identity from the government when exercising his freedom of expression.[160] This expectation of privacy is undermined when the government surreptitiously uses an IMSI catcher to identify every person at, for instance, a political rally, or a meeting of the NAACP, or an Alcoholics Anonymous meeting. The ability of the government to unrestrainedly use an IMSI catcher would almost certainly chill or dissuade certain activities. How likely would a person be to attend a strip club or an appointment at Planned Parenthood if she thought the government was recording every person who entered? Accordingly, deploying an IMSI catcher under such circumstances for the purpose of identifying the mobile phones within a particular area invades a significant privacy interest.[161] As such, it should not occur without a warrant. And courts should carefully consider whether such capabilities are even permissible with a warrant, given the rights of expression and association on which they may impinge.

---

[157] *Cf. Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring) ("And because GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: 'limited police resources and community hostility.'" (citation omitted)).

[158] *See* Bates v. City of Little Rock, 361 U.S. 516 (1960) (holding city could not criminalize the failure to reveal membership lists); NAACP v. Alabama, 357 U.S. 449 (1958) (holding the NAACP need not disclose its membership lists to Alabama).

[159] *See* McIntyre v. Ohio Elections Comm'n, 514 U.S. 334 (1995) (protecting distribution of anonymous campaign literature); Talley v. California, 362 U.S. 60 (1960) (striking down ordinance that prohibited the distribution of anonymous handbills).

[160] *See, e.g.*, Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L.J. 213, 274–75 (2002) (persuasively arguing that a concern for anonymity should be a consideration when determining if the Fourth Amendment applies).

[161] The invasion is made even more troubling by the fact that the government can operate IMSI catchers in secret, without making their targets aware of the surveillance. There is no organization, like the NAACP, to push back against the disclosure of its membership list. The lack of this additional check on government intrusion makes it even more crucial that police forces and others be forced to seek court approval before using an IMSI catcher.

Even where deployment of an IMSI catcher is unlikely to ensnare those engaged in protected expression or associational activities, it is questionable whether the government should be allowed to obtain the IMSIs of a large number of innocent people if its motivation is purely to prevent crime. As the Court recently reiterated in *Maryland v. King*, a search may be reasonable, even without a warrant, if the public interest is so substantial that it outweighs the privacy interests involved.[162] But, that public interest cannot merely be a "general interest in crime control" if a significant number of innocent people will be impacted by the search, in however small a fashion.[163] For instance, in *Maryland v. King*, the Court sanctioned a post-arrest cheek swab to obtain DNA from all arrestees because of the "significant government interest at stake in the identification of arrestees" and "the unmatched potential of DNA identification to serve that interest."[164] As the cases we discuss above indicate, however, IMSI catchers are being deployed for "crime control" purposes, that is, to identify or locate criminal suspects in the course of a criminal investigation—not merely to verify their identity once they have been arrested on probable cause. That crime control interest is not sufficient to outweigh the privacy of the numerous innocent persons that will be caught up in the IMSI catcher dragnet. Thus, as we discussed earlier, the lower courts are correct to be concerned about the innocent mobile phone users whose information may be obtained with IMSI catchers. At the least, such a concern should ensure that a warrant is required before an IMSI catcher is used. And that warrant should include safeguards designed to minimize or eliminate the impact on innocent mobile phone users.

As a final point on IMSI catchers, some might contend the act of obtaining an IMSI is not a search, thus not implicating many of the concerns we have discussed. In *Smith v. Maryland*, the Court ruled that the government's use of a pen register to obtain the phone numbers the defendant dialed was not a search because the defendant did not have a reasonable expectation of privacy in those numbers.[165] The Court's decision hinged on the fact that it considered it a well-known fact that the phone company must receive those numbers in order to appropriately route any call.[166] If the phone company had access to the numbers dialed, then the defendant could not reasonably consider them to be private. It is true that IMSIs are transmitted when a phone or other mobile device connects to

---

[162] Maryland v. King, 133 S. Ct. 1958, 1969 (2013).

[163] *See* City of Indianapolis v. Edmond, 531 U.S. 32, 38–44 (2000); *see also King*, 133 S. Ct. at 1981 (Scalia, J., dissenting) ("Even the common name for suspicionless searches—'special needs' searches—itself reflects that they must be justified, *always*, by concerns 'other than crime detection.'" (citations omitted)).

[164] *King*, 133 S. Ct. at 1977.

[165] *See* Smith v. Maryland, 442 U.S. 735, 745–46 (1979).

[166] *Id.* at 742–43 ("All telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed. . . . [I]t is too much to believe that telephone subscribers, under these circumstances, harbor any general expectation that the numbers they dial will remain secret.").

a network. But unlike the phone number the petitioner dialed in *Smith v. Maryland*, it cannot be reasonably said that most persons understand they are transmitting an IMSI every time they use their mobile phone. In fact, most mobile device users probably do not even know what an IMSI is, much less that it is conveyed as part of their phone use. At a more general level, it does not seem reasonable for a person to expect that merely by carrying his mobile phone around with him the government would at all times be able and free, without judicial restraint, to identify him and determine his location. It may be partly this consideration that caused the Southern District of Texas to refuse to consider an IMSI catcher as the functional equivalent of a pen register.[167] As Magistrate Judge Owsley pointed out, unlike a pen register where the police are tracking phone numbers dialed by an already identified phone number, here the police are trawling for the identification information as an initial matter, implicating Fourth Amendment concerns. This supports the view that the use of an IMSI catcher, even for identification purposes, should require a warrant.

C. *Mass Surveillance of the Network*

Finally, we consider the ability of governments to use mass surveillance technologies to intercept broad categories of information—both metadata and content—for later analysis. For the purpose of this discussion, we presume such interception constitutes a search. While we realize that is a large presumption, it is beyond the scope of this Article to analyze how each possible form of information that could be directly intercepted in mass surveillance might affect the question of whether the initial interception constitutes a search. Although, as we mention with regard to IMSI catchers, even if a person might not have a reasonable expectation of privacy in individual items of data obtained, capturing that information on the scale contemplated by mass surveillance may implicate the privacy concerns raised by Justices Alito and Sotomayor in their *Jones* concurrences.[168] As Justice Sotomayor so eloquently stated with regard to GPS monitoring:

> Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse. The net result is that GPS monitoring—by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track—may "alter the

---

[167] *See In re* The Application of the U.S. for an Order Authorizing the Installation and Use of a Pen Register and Trap and Trace Device, 890 F. Supp. 2d 747, 748 (S.D. Tex. 2012).

[168] *See supra* Part III.B.

> relationship between citizen and government in a way that is inimical to democratic society."[169]

The same can be said of mass surveillance, which has the potential to reveal even more detail than locational tracking.[170]

Presuming mass surveillance constitutes a search, therefore, it is hard to see how it could be reasonable. As we discussed with regard to IMSI catchers, the Court has repeatedly emphasized that searches that are not tied to individualized suspicion are rarely consistent with the Fourth Amendment.[171] These "special needs" searches cannot be justified by a "general interest in crime control."[172] But rather, as in *Maryland v. King*, a search must be motivated by another significant government interest such as the identification of arrestees.[173] Mass surveillance, by its nature, cannot be justified by individualized suspicion. And unlike an IMSI catcher search, where steps might be taken to limit the impact on innocent mobile phone users, the whole purpose of mass surveillance is not to minimize the collection of information from innocents, but in fact to maximize it in case, sometime now or in the future, it might prove useful. This leads us to presume that mass surveillance based on a desire to prevent crime is not consistent with the Fourth Amendment.

As we noted at the beginning of this section, recent attention on U.S. intelligence activities raises the question of whether such directed mass surveillance might be justified on national security grounds. With regard to domestic surveillance, the Court has held that a national security purpose does not exempt such surveillance from the Fourth Amendment's requirements.[174] In fact, domestic national security surveillance may even heighten certain privacy concerns, as explained by the Court: "Fourth Amendment protections become the more necessary when the targets of official surveillance may be those suspected of unorthodoxy in their political beliefs. The danger to political dissent is acute where the Government attempts to act under so vague a concept as the power to protect 'domestic security.'"[175] For these reasons, we think courts should tread carefully when considering whether national security is a sufficient justification for mass surveillance.

---

[169] United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring) (citation omitted).

[170] For a persuasive argument as to why *Smith v. Maryland* is inapplicable in the mass surveillance context, even where collection of metadata is involved, see the ACLU's Memorandum of Law in Support of Plaintiffs' Motion for a Preliminary Injunction, *supra* note 113, at 21–23.

[171] *See* Chandler v. Miller, 520 U.S. 305, 308–09 (1997).

[172] *See* City of Indianapolis v. Edmond, 531 U.S. 32, 38–44 (2000); *see also* Maryland v. King, 133 S. Ct. 1958, 1981–82 (2013) (Scalia, J., dissenting).

[173] *King*, 133 S. Ct. at 1970.

[174] *See* United States v. U.S. Dist. Court for the E. Dist. of Mich., 407 U.S. 297, 321–22 (1972) (holding that a search warrant is required when wiretapping in the interest of national security).

[175] *Id.* at 314.

IV. CONCLUSION

We are in need of a reconceptualization of modern surveillance powers. Inasmuch as we still consider "interception" as the tapping of a line outside of someone's home,[176] we still believe that surveillance is as targeted in design as it is in implementation. Neither is necessarily true anymore. Even the emphasis in the literature on the "third party doctrine" may require re-thinking, as it presumes that modern surveillance requires third party Internet companies and telephony providers. As we see with the technologies reviewed in this Article, the human is no longer necessarily the observer nor the identified target within modern surveillance. An individual may be placed under communications surveillance because of his or her location (e.g., near an IMSI catcher), virtual address (e.g., on the same stream of communications as someone else or using the same IP address or computer that is then attacked with a Trojan), or characteristics (e.g., same spoken language, similar topic of conversation). The surveillance may be authorized because of these characteristics, not because a known individual is using a particular communications medium. Such practices only increase the need for legal safeguards to protect our privacy.

Technological change has long been compelling us to rethink the application of our constitutional values. In theory, Parliaments and Congresses could act to regulate these technologies, to place them under strict rules. They have, to date, failed to do so. Instead, we are seeing that the courts are exploring these questions around new communications surveillance techniques. Our analysis, based on Supreme Court decisions regarding the Fourth Amendment, recommends that the courts establish strong boundaries around these new investigative techniques.

[176] Or in the case of Katz, the bugging of a specific telephone booth.