TRADEMARKS AS SURVEILLANCE TRANSPARENCY

Amanda Levendowski†

ABSTRACT

We know very little about the technologies that watch us. From cell site simulators to predictive policing algorithms, the lack of transparency around surveillance technologies makes it difficult for the public to engage in meaningful oversight. Legal scholars have critiqued various corporate and law enforcement justifications for surveillance opacity, including contract and intellectual property law. But the public needs a free, public, and easily accessible source of information about corporate technologies that might be used to watch us. To date, the literature has overlooked a free, extensive, and easily accessible source of information about surveillance technologies hidden in plain sight: federal trademark filings.

This Essay examines the powerful and unexplored role of trademark law in exercising oversight within and beyond surveillance. Trademark law promotes access to information, and the process for federal registration of trademarks—long overlooked by scholars—demands extensive public disclosures that reveal a wealth of information about surveillance technologies. This Essay leverages examples from real trademark applications to explore how journalists, researchers, and civil society can use the detailed disclosures in trademark applications for transparency. I conclude that trademark law can be a powerful tool for correcting longstanding information asymmetries between the watchers and the watched by empowering the public to watch back.

DOI: https://doi.org/10.15779/Z38VT1GQ6P

† Associate Professor of Law, Georgetown University Law Center. Thanks to Lindsey Barrett, Barton Beebe, Hannah Bloch-Wehba, Priya Chadha, Julie Cohen, Bradley Girard, Dave Gershorn, Thomas Haley, Alex Reeve Givens, Megan Graham, Woody Hartzog, Brett Max Kaufman, Christina Koningisor, Marty Lederman, Karen Levy, Naomi Mezey, Mark McKenna, Chris Morten, Laura Moy, Jennifer Rothman, Matthew Sag, Madelyn Sanfillipio, Jessica Silbey, Ed Timberlake, Rebecca Tushnet, Jacob Victor, Ari Waldman, Rebecca Wexler, and Cameron Tepski for their thoughtful and generous comments. This Essay benefited from presentation at the Georgetown Tech Law Scholar Seminar, Privacy Law Scholars Conference, Junior Law and Tech* Scholars Workshop, and Georgetown Faculty Workshop. Shadé Oladetimi provided sharp research assistance.

TABLE OF CONTENTS

I. INTRODUCTION

In February 2018, Amazon acquired a "smart" doorbell company called Ring.[1] For Amazon, a company that delivers more than 5 billion items annually,[2] acquiring a way to monitor the real estate where packages get delivered makes sense. Yet statements from the acquired Ring seemed grandiose for the purchase of a private security system, including that the company "look[ed] forward to being a part of the Amazon team as we work toward our vision for safer neighborhoods."[3] Amazon's full vision for Amazon Ring devices became clear to the public more than a year later when journalists revealed that the company had quietly partnered with police departments

1. Laura Stevens & Douglas MacMillan, *Amazon Acquires Ring, Maker of Video Doorbells*, WALL ST. J. (Feb. 27, 2018), https://www.wsj.com/articles/amazon-acquires-ring-maker-of-video-doorbells-1519768639.

2. Ashley Carman, *Amazon Shipped over 5 Billion Items Worldwide Through Prime in 2017*, THE VERGE (Jan. 2, 2018), https://www.theverge.com/2018/1/2/16841786/amazon-prime-2017-users-ship-five-billion.

3. Eugene Kim, *Amazon Buys Smart Doorbell Maker Ring for a Reported $1 Billion*, CNBC (Feb. 27, 2018), https://www.cnbc.com/2018/02/27/amazon-buys-ring-the-smart-doorbell-maker-it-backed-through-alexa-fund.html.

across the country to promote and deploy Amazon Ring devices as part of a privatized surveillance network.[4]

Private companies, like Amazon, increasingly create surveillance technology used by law enforcement, but the public is often not aware that these technologies are being developed and deployed until the technology is already embedded in communities. Private companies developing surveillance technology for law enforcement is not new, and neither is the lack of transparency around those relationships. Acquisitions of surveillance technology may be made with outside funding or through in-kind donations to police departments, making surveillance technology difficult to track through financial disclosures.[5] Filing federal Freedom of Information Act (FOIA) requests or using local public records laws to ask for information about surveillance technologies used by law enforcement is, as Hannah Bloch-Wehba has highlighted, resource intensive and lacks any guarantee that law enforcement will disclose responsive documents about surveillance technology.[6] Elizabeth Joh has detailed how private contracts, such as non-

4. Caroline Haskins, *Amazon Requires Police to Shill Surveillance Cameras in Secret Agreement*, MOTHERBOARD (July 25, 2019), https://www.vice.com/en_us/article/mb88za/amazon-requires-police-to-shill-surveillance-cameras-in-secret-agreement; Dell Cameron, *Amazon's Ring Barred Cops From Using 'Surveillance' to Describe Its Products*, GIZMODO (Aug. 19, 2019), https://gizmodo.com/ring-barred-cops-from-using-surveillance-to-describe-it-1837380102; Drew Harwell, *Doorbell-Camera Firm Ring Has Partnered with 400 Police Forces, Extending Surveillance Concerns*, WASH. POST (Aug. 28, 2019), https://www.washingtonpost.com/technology/2019/08/28/doorbell-camera-firm-ring-has-partnered-with-police-forces-extending-surveillance-reach/?noredirect=on. Earlier this year, the House Subcommittee on Economic and Consumer Policy sent a letter to Amazon requesting detailed information about partnerships between Amazon Ring and law enforcement. *See* Letter from Raja Krishnamoorthi, Chairman, H. Subcomm. on Econ. & Consumer Pol., to Brian Huseman, Vice President of Pub. Pol'y, Amazon.com, Inc. (Feb. 19, 2020), https://oversight.house.gov/sites/democrats.oversight.house.gov/files/2020-02-19.RK%20to%20Huseman-Amazon%20re%20Ring%20%281%29.pdf.

5. Laura Nahmais, *Police Foundation Remains a Blind Spot in NYPD Contracting Process, Critics Say*, POLITICO (July 13, 2017), https://www.politico.com/states/new-york/city-hall/story/2017/07/13/police-foundation-remains-a-blind-spot-in-nypd-contracting-process-critics-say-113361. Thanks to Rashida Richardson for this observation.

6. Hannah Bloch-Wehba, *Access to Algorithms*, 88 FORDHAM L. REV. 1265, 1296–1303 (2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3355776; *see also*, Order denying permissibility of Glomar response with regard to documents requested by protestors, *Millions March NYC v. N.Y. City Police Dep't*, Index No. 100690 (Jan. 14, 2019), https://assets.documentcloud.org/documents/5684730/Nypd-Foil.pdf (denying New York City Police Department's Glomar response withholding responsive documents regarding surveillance technology used during protests); *infra* Part II. For a thorough examination of the shortcomings of FOIA requests, see generally Nathan Freed Wessler, "*[We] Can Neither Confirm Nor Deny the Existence or Nonexistence of Records Responsive to Your Request": Reforming the Glomar Response to FOIA*, 85 N.Y.U. L. REV. 1381 (2010).

disclosure agreements between police departments and surveillance technology companies, can pose another roadblock to transparency.[7] And Rebecca Wexler and Sonia Katyal have likewise documented the ways in which trade secret law can operate to shield surveillance technology from public scrutiny.[8] Some jurisdictions have responded to this disparity by enacting procurement policies for surveillance technologies, as Catherine Crump has examined, but few jurisdictions have enacted policies that require public disclosure of a proposed surveillance technology prior to procurement.[9] Taken together and put into practice, these hurdles look like invoking non-disclosure agreements to avoid judicial scrutiny of surveillance technology,[10] incentivizing companies to collect and sell personal information without consent or notice,[11] and shielding surveillance algorithms from independent review or oversight.[12] The reasons vary, but the result is the same: there is a vast informational inequity between law enforcement and the public about surveillance technologies.[13]

Journalists and civil society have turned to other public sources of information, such as Securities and Exchange Commission disclosures and patent filings, to help correct these disparities.[14] But SEC disclosures are often too general to reveal useful information about surveillance technology products.[15] And patent filings are not a promise to produce a product, as

7. Elizabeth E. Joh, *The Undue Influence of Surveillance Technology Companies on Policing*, 92 N.Y.U. L. REV. 101 (2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2924620.

8. Rebecca Wexler, *Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System*, 70 STAN. L. REV. 1343 (2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2920883; Sonia Katyal, *The Paradox of Source Code Secrecy*, 104 CORNELL L. REV. 1183 (2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3409578.

9. Catherine Crump, *Surveillance Policy Making by Procurement*, 90 WASH. L. REV. 1596 (2016), https://scholarship.law.berkeley.edu/facpubs/2633/; *see also* Ira Rubinstein, *Privacy Localism*, 93 WASH. L. REV. 1961 (2018), https://digitalcommons.law.uw.edu/wlr/vol93/iss4/8/ (discussing procurement policies in Seattle, Washington and New York, New York).

10. *See infra* Part III.A (discussing Harris Corporation's Stingray devices).

11. *See infra* Part III.B (discussing Vigilant Solutions' automated license plate readers).

12. *See infra* Part III.C (discussing PredPol's predictive policing algorithms).

13. *See infra* Part III (discussing asymmetries between public awareness of law enforcement surveillance technologies and law enforcement's use of those technologies).

14. *See, e.g.*, AMAZON, ANNUAL REPORT (FORM 10-K) 51–2 (Dec. 31, 2018), https://www.sec.gov/Archives/edgar/data/1018724/000101872419000004/amzn-20181231x10k.htm (using K-filings to investigate Amazon); Generating Composite Facial Images Using Audio/Video Recording and Communications Devices, U.S. Patent Application No. 15/984,298, Publication No. 20180341835 (published Nov. 29, 2018)(Amazon Technologies, Inc., applicant), https://www.aclunc.org/docs/Amazon_Patent.pdf (using patent filings to investigate Amazon).

15. *See, e.g.*, AMAZON, *supra* note 14, at 51–2 (disclosing that Ring Inc. was purchased "for cash consideration of approximately $839 million" for the primary reason, along with

Amazon pointed out when confronted with a patent filing for a Ring-compatible expansion that would enable the cameras to create composite images of people to incorporate into a "database of suspicious persons."[16]

Taken together, surveillance transparency has never been more challenging. If there is hope for resistance—including public discussion or dialogue—before law enforcement embraces secret surveillance technologies, the public desperately needs a freely available, easily accessible source of information about the technologies that will be used to watch us.[17] One source is consistently overlooked: federal trademark filings.

Take Amazon Ring. In its August 2018 trademark application for the AMAZON RING mark, Amazon publicly revealed its vision for Ring: "[a]utomated self-contained electronic surveillance that can be deployed to

other acquisitions, of "acquir[ing] technologies and know-how to enable Amazon to serve customers more effectively").

16. Generating Composite Facial Images Using Audio/Video Recording and Communications Devices, U.S. Patent Application No. 15/984,298, Publication No. 20180341835 (Published Nov. 29, 2018) (Amazon Technologies, Inc., applicant), https://www.aclunc.org/docs/Amazon_Patent.pdf; *see also* Peter Holley, *This Patent Shows Amazon May Seek to Create a 'Database of Suspicious Persons' Using Facial-Recognition Technology*, WASH. POST, (Dec. 18, 2018), https://www.washingtonpost.com/technology/2018/12/13/this-patent-shows-amazon-may-seek-create-database-suspicious-persons-using-facial-recognition-technology/; Jacob Snow, *Amazon's Disturbing Plan to Add Face Surveillance to Your Front Door*, ACLU: SPEAK FREELY BLOG, (Dec. 12, 2018), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-disturbing-plan-add-face-surveillance-yo-0. For an accounting of why technology companies continue to file for dystopian patents, see generally Janet Freilich, *Prophetic Patents*, 53 U.C. DAVIS L. REV. 663 (2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3202493 (examining patents that contain fictional data); Rose Eveleth, *Why Are There So Many Weird Tech Patents?*, SLATE, (Aug. 28, 2019), https://slate.com/technology/2019/08/amazon-sony-facebook-strange-patents.html (assessing the incentives that fuel hypothetical patents).

17. Surveillance technology is disproportionately deployed against people with limited political power. For a detailed accounting of the ways in which U.S. surveillance is deeply rooted in anti-Blackness, see generally SIMONE BROWNE, DARK MATTERS: ON THE SURVEILLANCE OF BLACKNESS (2015). American surveillance expanded quickly to include many other marginalized people, including immigrants, religious minorities, and poor and working people. For an accounting of how past and present practices of the American law enforcement surveillance apparatus affect each in turn, see generally GEORGETOWN LAW: CENTER FOR PRIVACY AND TECHNOLOGY, COLOR OF SURVEILLANCE, https://www.law.georgetown.edu/privacy-technology-center/events/color-of-surveillance-2017 (last visited Nov. 19, 2020).

gather evidence or intelligence."[18] And it did so nearly a year before journalists detailed how that vision would operate in practice.[19]

Federal trademark filings can offer important insight into the surveillance technologies that private corporations are developing, but the public has not fully explored the Trademark Electronic Search System (TESS) and Trademark Status and Document Retrieval (TSDR) databases as joint pathways toward surveillance transparency.[20] The reason is obvious. As Justice Samuel Alito observed, "[I]t is unlikely that more than a tiny fraction of the public has any idea what federal registration of a trademark means."[21]

This is, in some part, attributable to the dearth of scholarly writing related to the federal trademark registration process. As recently as 2017, Rebecca Tushnet observed that the mechanics of trademark registration garner little attention—and not much has changed in the interim years.[22] This Essay delves

18. AMAZON RING, U.S. Trademark Application Serial No. 88075713, TEAS RF New Application at 5 (filed Aug. 13, 2018).

19. *Compare* Amanda Levendowski, *How Can We Learn About the AI Systems That Might Be Used to Surveil Us? The Federal Trademark Register Has Answers*, AI ETHICS INITIATIVE: GUEST BLOGGER (Oct. 11, 2018), https://aiethicsinitiative.org/news/2018/10/11/guest-blogger-amanda-levendowski-how-can-we-learn-about-the-ai-systems-that-might-be-used-to-surveil-us-the-federal-trademark-register-has-answers (published less than a month after the trademark application for the AMAZON RING mark was filed), *with* Caroline Haskins, *Amazon Requires Police to Shill Surveillance Cameras in Secret Agreement*, VICE MOTHERBOARD (July 25, 2019), https://www.vice.com/en_us/article/mb88za/amazon-requires-police-to-shill-surveillance-cameras-in-secret-agreement (revealing program discovered via public records requests requiring local law enforcement to "[e]ngage the Lakeland community with outreach efforts on the platform to encourage adoption of the platform/app"), *and* Drew Harwell, *Doorbell-Camera Firm Ring Has Partnered with 400 Police Forces, Extending Surveillance Concerns*, WASH. POST (Aug. 28, 2019), https://www.washingtonpost.com/technology/2019/08/28/doorbell-camera-firm-ring-has-partnered-with-police-forces-extending-surveillance-reach (detailing hundreds of partnerships between Amazon Ring and local law enforcement offering discounts to cities and community groups that invest public or taxpayer-supported funds on Amazon Ring devices and potentially grant access to civilians' home devices).

20. There are also 50 state trademark registers, each with their own rules and procedures and processes, and international registers, some of which are accessible online. *See, e.g.*, *eSearch Plus*, EUR. UNION INTELL. PROP. OFF., https://euipo.europa.eu/eSearch/ (last visited Jan. 5, 2020) (search database for European Union trademarks, designs, owners, representatives, Bulletins, and Office decisions); *TMview*, EUR. UNION INTELL. PROP. OFF., https://www.tmdn.org/tmview/welcome (last visited Jan. 5, 2020) (database of trademark names, applications, and registration numbers in additional countries and databases).

21. Matal v. Tam, 137 S. Ct. 1744, 1759 (2017) (citing Application of Nat'l Distillers & Chem. Corp. 49 C.C.P.A. 854, 863 (1962) (Rich, J., concurring)).

22. Rebecca Tushnet, *Registering Disagreement: Registration in Modern American Trademark Law*, 130 HARV. L. REV. 867, 870–71 (2017), http://harvardlawreview.org/wp-content/uploads/2017/01/867-941-Online-updated.pdf ("Foundational critiques of modern trademark law tend not to address the role of registration. . . . Proponents of the Chicago School of law and economics approach, whose account of the function of trademark as

into the largely unexamined mechanics of the federal trademark registration process and analyzes how the process of federally registering trademarks compels companies to disclose details about new surveillance technologies. In so doing, this Essay's goal is to offer a new tool in the quest for surveillance transparency and to equip the public, including journalists, researchers, and civil society, with the skills necessary to investigate trademark records for themselves.

The Essay proceeds in two parts. Part II describes the process for federal registration of trademarks and identifies three portions of trademark filings that are likely to disclose information about surveillance technology: the stated basis for use, the goods and services description, and the specimen. Part III uses the applications for registration of trademarks for three surveillance technologies—Harris Corporation's STINGRAY cell site location information (CSLI) interceptor, Vigilant Solution's VIGILANT SOLUTIONS automated license plate reader, and Predpol's PREDPOL predictive policing software—to illustrate how to leverage revealing disclosures in trademark filings for transparency. This Essay concludes that federal trademark filings are a freely available, easily accessible way for the public to learn about surveillance technologies used to watch us.

II. DISCOVERING DISCLOSURES IN TRADEMARK FILINGS

A trademark is "any word, name, symbol, device, or any combination" of those things that can be used to identify the provider or seller, and indicate the source, of certain goods and services.[23] As the Supreme Court has observed, "[f]ederal law does not create trademarks."[24] Rather, it is the seller's use of a mark that creates a trademark which grants some enforceable rights.[25] The reality remains, however, that federal trademark registration confers crucial rights and benefits, such as providing constructive notice of the registrant's

reducing consumers' search costs is now dominant, likewise have little to say about registration. . . . American scholars, in sum, have often treated registration like a borrowed civil law coat thrown awkwardly over the shoulders of a common law regime.").

23. *Trademark Basics*, U.S. PAT. & TRADEMARK OFF., https://www.uspto.gov/trademarks-getting-started/trademark-basics (last visited Sept. 22, 2019).

24. *Matal*, 137 S. Ct. at 1751 (quoting *B&B Hardware, Inc. v. Hargis Indus.*, 575 U.S. 138, 142 (2015)).

25. *See, e.g.*, 15 U.S.C. § 1125 (protecting qualifying unregistered marks from infringement, dilution, and tarnishment); *see also* 15 U.S.C. § 1125(d) (protecting qualifying unregistered marks from cybersquatting).

claim of ownership and offering prima facie evidence that the registered mark is valid.[26]

There is ample scholarship exploring the purposes of trademark law.[27] But as Rebecca Tushnet has explained, precious little of that scholarship details the mechanics of federal trademark registration.[28] Indeed, to date, there has been no scholarship centered on the mechanics of investigating federal trademark filings.

The federal trademark registration process begins, somewhat circuitously, with an application to register a trademark.[29] An applicant discloses detailed information about the mark they are seeking to register, including whether the mark has been used, the sorts of goods and services on which the mark is (or will be) used, and, in some instances, a depiction of how the mark is (or will be) used in the real world.[30] Federal trademark filings are all freely and publicly

26. *Matal*, 137 S. Ct. at 1753 (quoting *B&B Hardware*, 575 U.S. 138, 142) (detailing additional benefits of federal registration). Owners of a federally registered trademark can also prevent importation of items bearing an infringing mark into the United States. *See* 15 U.S.C. § 1124. The tremendous value of a trademark registration explains why, despite having to reveal information about secretive surveillance technologies, companies continue to seek federal trademark registrations for their marks.

27. *See, e.g.*, William M. Landes & Richard A. Posner, *Trademark Law: An Economic Perspective*, 30 J. LAW & ECON. 265, 296 (1987) (advocating an economic theory of trademark law); Barton Beebe, *The Semiotic Analysis of Trademark Law*, 51 UCLA L. REV. 621, 669 (2004) (advancing a semiotic theory underlying trademark law); Mark P. McKenna, *The Normative Foundations of Trademark Law*, 82 NOTRE DAME L. REV. 1839 (2007) (examining multiple theories of trademark law, including preventing trade diversion, protecting consumers, and the shift toward protecting marks qua marks).

28. *See* Rebecca Tushnet, *Registering Disagreement: Registration in Modern American Trademark Law*, 130 HARV. L. REV. 867, 870–71 (2017).

29. *See* Kelly Servs. v. Creative Harbor, LLC, 846 F.3d 857, 876 (6th Cir. 2017) (Batchelder, J., dissenting), https://www.leagle.com/decision/infco20170123094 (providing perhaps the most complete judicial discussion of the trademark application and registration process).

30. *See generally*, *Apply Online*, U.S. PAT. & TRADEMARK OFF., https://www.uspto.gov/trademarks-application-process/filing-online (last visited Nov. 20, 2020) (outlining the forms necessary to apply for a federal trademark online). The revealing disclosures demanded by the federal trademark application process incentivize some companies to take advantage of the closed, non-public registers of countries like Trinidad and Tobago—or to use shell companies, as was the case with the AMAZON RING filing—to protect their mark without disclosing detailed information to the public about products or services in development. *See* AMAZON RING, U.S. Trademark Application Serial No. 88075713 (filed on Aug. 13, 2018 by "A9.com, Inc." and later assigned to Amazon Technologies, Inc. on May 15, 2019). These methods allow a company to claim priority of the earlier foreign filing without disclosing details about the mark—or the mark itself—until months later. For a detailed analysis of these so-called "submarine trademarks," see generally CARSTEN FINK, ANDREA FOSFURI, CHRISTIAN HELMERS & AMANDA MYERS, *Submarine Trademarks*, NORTHWESTERN PRITZKER SCHOOL OF

searchable using the TESS. The U.S. Patent and Trademark Office (USPTO) launched TESS in 2000.[31] TESS offers a way to search federal trademark filings online without cost but, while it does not require any technical expertise, it can be a tricky interface.

There are two primary types of TESS searches: simple and structured.[32] Using the basic fields in both types of searches, enquirers can surface trademark applications for surveillance technologies through strategic queries. Simple searches enable searching by limited criteria, namely by Combined Word Mark (e.g., AMAZON RING), Serial or Registration Number (88075713), and Owner Name and Address (Amazon Technologies, Inc., 410 Terry Avenue North, Seattle, Washington 98109).[33] Structured searches permit searching by a wider range of search terms across many more fields, including Current Basis (1B, Intent to Use), Goods and Services (surveillance), and International Class (Class 9).[34] After running a search using TESS, one can view each of the filings for a particular application for registration of a trademark using the TSDR system.[35]

Crucially, and unlike patent applicants, all federal trademark applicants must make "bona fide use of the mark in the ordinary course of trade, and not made merely to reserve a right in a mark" before the Examiner will allow a mark to be added to the Principal or Supplemental Register.[36] Applicants who make misrepresentations during the trademark application process risk losing

---

LAW (Feb. 15, 2019), http://www.law.northwestern.edu/research-faculty/clbe/events/innovation/documents/helmers_submarine_trademarks.pdf.

31. *USPTO Introduces New Trademark Electronic Search System*, U.S. PAT. & TRADEMARK OFF., https://www.uspto.gov/about-us/news-updates/uspto-introduces-new-trademark-electronic-search-system (last visited Oct. 22, 2019); *see also* Barton Beebe & Jeanne C. Fromer, *Are We Running Out of Trademarks? An Empirical Study of Trademark Depletion and Congestion*, 131 Harv. L. Rev. 945, 970–71 (2018) (discussing the origins of TESS).

32. *Trademark Electronic Search System*, U.S. PAT. & TRADEMARK OFF., http://tmsearch.uspto.gov. (last visited Oct. 22, 2019). The third type of search, free form, permits the construction of searches using Boolean logic across multiple search fields. *See id.*

33. *Id.*

34. *Id.*; *see infra* Parts II.A–C.

35. There are many acronyms involved in the process to federally register a trademark. *See Trademark Status and Document Retrieval (TSDR)*, U.S. PAT. & TRADEMARK OFF., http://tsdr.uspto.gov/. Note that there are far fewer ways to run trademark searches using TSDR, which limits search fields to US Serial, Registration, or Reference number or International Registration number. *Id.*

36. 15 U.S.C. § 1127; *see also* U.S. PAT. & TRADEMARK OFF., TRADEMARK MANUAL OF EXAMINING PROCEDURE § 901.02 (Oct. 2018), https://tmep.uspto.gov/RDMS/TMEP/current#/Oct2018/TMEP-900d1e7.html [hereinafter TMEP]. Note that there are special provisions for marks registered internationally. *See, e.g.*, 15 U.S.C. § 1126; 15 U.S.C. § 1141(f).

federal trademark protection for their mark.[37] Requiring that applicants must intend to use the mark in connection with the goods and services identified in the application for registration means that applications for registration of trademarks avoids the issue created by dystopian patents that companies, like Amazon, dismiss as speculative.[38] Instead, the bona fide requirement forces companies to stand by representations made in their applications, correct their errors or admit to misleading the USPTO.

Three portions of the applications to register trademarks predictably yield useful information about surveillance technologies. The first is the "use designation," which requires the applicant to identify whether the application for registration is based on use of the mark for the underlying product or whether the application is based on an intent to use the mark.[39] The second is the goods and services classifications and descriptions, which offer general categorizations and specific identifications of the types of products for which the mark will be used. And the final one, and perhaps the most unique and valuable, is the "specimen" portion, which consists of visual representations depicting how the mark is used in commerce—think screenshots of computer interfaces and photographs of hardware emblazed with logos. This Part examines each of those three portions of trademark applications in turn.

A. INTENT TO USE OR IN-USE DESIGNATION

Federal trademark filings require a designation regarding whether the owner currently uses the mark in commerce or whether the owner intends to use the mark at a future date.[40] When viewing an application in TESS, these designations are coded as filing bases 1A and 1B, respectively.[41] For in-use applications, the owner must disclose the date the mark was first used in commerce.[42] The use designation offers a way to determine when goods and

37. *See, e.g.*, Nationstar Mortgage LLC v. Ahmad, 112 U.S.P.Q.2d 1361 (T.T.A.B. 2014) (sustaining fraud claim and refusing to register NATIONSTAR mark).

38. *See supra* Part I.

39. The mark need not be in use at the time of the filing, so long as the use designation is identified as "intent-to-use." *See* TMEP, *supra* note 36, § 1101.

40. 15 U.S.C. § 1051(a)–(b).

41. The 1A and 1B designations are named after the sections of the Lanham Act that govern federal trademark applications. *See* 15 U.S.C. § 1051(a)–(b). The intent-to-use designation was introduced by the Trademark Law Revision Act of 1988. Pub. L. No. 100-667, 15 U.S.C. § 1051(b) (1988). For skepticism about whether intent-to-use applications were an ill-advised addition to the Lanham Act, see generally Amy B. Cohen, *Intent to Use: A Failed Experiment?*, 35 U.S.F. L. REV. 683 (2001).

42. 15 U.S.C. § 1051(a)(2). Six months after filing an intent-to-use application, the owner must file a Statement of Use confirming that the mark is being used in commerce or risk abandoning the application. 15 U.S.C. § 1051(d)(1). On a showing of good cause by the applicant, the Director of the U.S. Patent and Trademark Office may grant a series of six-

services under a particular mark were first offered to the relevant purchasing public, which, in some instances, may be sales to law enforcement.

B. GOODS AND SERVICES CLASSIFICATIONS AND DESCRIPTIONS

The goods and services classification and description portion of federal trademark filings consists of two components: a numerical classification categorizing the goods or services and a plain-language description of the goods or services to be covered by a particular mark.[43] The classification and description requirement for federal trademark filings dates back to 1870 and the earliest codified trademark law in the United States, which required applicants to identify "the class of merchandise and the particular description of goods comprised in such class, by which the trademark has been or is intended to be appropriated."[44] Subsequent trademark laws similarly required the identification of goods, although without acknowledging protection for federal trademarks used in connection with services.[45] The Lanham Act, passed in 1946, finally extended trademark protection to services.[46]

Federal law does not mandate a classification system, but the Director of the USPTO has determined one:[47] the Nice Classification, a numerical classification system featuring 45 distinct classes, with so-called International Classes 1 through 34 identifying goods and International Classes 35 through

---

month extensions, so long as the overall extension does not exceed 24 months. 15 U.S.C. § 1051(d)(2); *Trademark Applications—intent-to-use (ITU)* basis, U.S. PAT & TRADEMARK OFF., https://www.uspto.gov/trademarks-application-process/filing-online/intent-use-itu-applications (last visited Nov. 30, 2020).

43. *See* TMEP, *supra* note 36, 1401.02(a).

44. The Act ironically made no mention of trademark in its title but was rather intended to "revise, consolidate, and amend the statutes relating to patents and copyrights." H.R. 1714, 41st Cong. (1870). The first U.S. trademark law was struck down as unconstitutional after *The Trade-Mark Cases* in 1879, when the Supreme Court held that the Copyright Clause of the Constitution did not give Congress the power to protect or regulate trademarks. *See The Trade-Mark Cases*, 100 U.S. 82 (1879). Subsequent trademark laws were enacted under the authority of the Commerce Clause. *See* TMEP, *supra* note 36, § 1401.02(a).

45. *See, e.g.*, 1881 Trademark Bill; H.R. 16560, 58th Cong. (1905) (authorizing the registration of trademarks).

46. *See* Lanham Act of 1946, ch. 540, 60 Stat. 427; *see also In re Dr. Pepper Co.*, 836 F.2d 508, 509 (Fed. Cir. 1987) (holding a contest to promote the sale of one's goods is not a "service" within the meaning of the Latham Act).

47. 15 U.S.C. § 1112; TMEP, *supra* note 36, § 1401.02(a). Classifications are also the primary basis for determining registration fees for federal trademark applications, with each class costing between $225 and $400 depending on the type of trademark application. *Overview of Trademark Fees*, U.S. PAT. & TRADEMARK OFF., https://www.uspto.gov/trademark/fees-payment-information/overview-trademark-fees (last visited Oct. 28, 2019); TMEP, *supra* note 36, § 1401.01.

45 identifying services.[48] Class 1, for example, covers "chemicals," including those used in industry, science, photography, agriculture, and forestry, among many others.[49]

Surveillance technologies are likely to fall into one or more of the following classes: Class 9 covering electrical and scientific apparatuses, which includes hardware and computer software (such as body-worn cameras[50] or predictive policing algorithms), Class 42 covering computer and scientific services (such as developing big data analytics software), or Class 45 covering personal and legal services (such as surveillance services or monitoring computer services for clients).[51] Goods and services descriptions offer additional detail about the goods or services on which a mark will be used. Many model goods and services descriptions are included in the Acceptable Identification of Goods and Services Manual (ID Manual),[52] which operates as a guide for trademark applicants looking to craft goods and services descriptions that will be intelligible to trademark examiners and thus unlikely to create complications for the application.[53] Applicants may try to disclose limited information in goods and services descriptions, but such strategies may limit the power of the

48. TMEP, *supra* note 36, § 1401.02(a); *see also* the Nice Agreement (establishing a classification of goods and services for purposes of registering trademarks and service marks). The United States became a signatory to the Nice Agreement in 1973. *See* TMEP, *supra* note 36, § 1401.02(a).

49. TMEP, *supra* note 36, § 1401.02(a).

50. Taser International filed a trademark application for the AXON AI mark covering "[s]urveillance services featuring use of video cameras that can be worn on the head and the body and video surveillance systems used in automobiles, and computers and mobile electronic devices to provide location-specific information about the video" on February 20, 2017—more than 40 days before the rebrand from Taser to Axon was made public, teasing the company's increasing focus on software rather than hardware. *Compare* AXON AI, U.S. Trademark Application Serial No. 87341984 (filed Feb. 20, 2017), *with* Stephen Nellis, *Taser Changes Name to Axon in Shift to Software Services*, REUTERS (Apr. 5, 2017), https://www.reuters.com/article/us-usa-taser/taser-changes-name-to-axon-in-shift-to-software-services-idUSKBN177265.

51. TMEP, *supra* note 36, § 1401.02 (a). Other possible, though less likely, classes for surveillance technologies include Class 35 covering advertising and business services, Class 38 covering telecommunications services, and Class 41 covering education and entertainment services. *Id.*

52. *See Trademark ID Manual, ID Master List*, U.S. PAT. & TRADEMARK OFF., https://idm-tmng.uspto.gov/id-master-list-public.html (last visited Oct. 10, 2019). The ID Manual can be used to identify how particular goods and services related to surveillance are likely to be phrased. Those phrases can then be searched using TESS.

53. TMEP, *supra* note 36, § 1402.04. Applicants may create their own goods and services descriptions, but trademark examiners may take issue with the specificity of the description or disagree that a particular description is consistent with the identified class. In that case, the examiner may issue an "Office Action" to the applicant suggesting revisions to the existing description or requesting revisions from the applicant. *See* TMEP, *supra* note 36, § 705.

mark and, in some instances, trigger Office Action requests from the Examiner seeking information about additional goods and services.[54]

Searches using classifications and goods and services descriptions are "structured" searches within TESS.[55] After selecting the option to begin a structured search, users can search by classification by typing the desired class number as the "Search Term" and selecting "International Class" as the field.[56] Because a search premised on class alone would likely return many irrelevant results, one can further filter the search by typing key words from the goods and services description, such as "surveillance," as the Search Term and selecting "Goods & Services" as the field.[57] This search method is likely to yield surveillance technologies that may be used by law enforcement, such as the AMAZON RING application.[58]

C. SPECIMENS

Trademark applications filed on an in-use basis must include a "specimen," meaning some kind of label, tag, packaging, or other display that shows the mark used in connection with every class described in the application.[59] Specimens are required because they "… show the manner in which the mark is seen by the public . . . [and] provide supporting evidence of facts recited in

54. *See generally* TMEP, *supra* note 36, § 705.

55. *See Trademark Electronic Search System* (*TESS*), U.S. PAT. & TRADEMARK OFF., http://tmsearch.uspto.gov (last visited Oct. 10, 2019).

56. *Trademark Electronic Search System (TESS) Structured Search*, U.S. PAT. & TRADEMARK OFF., http://tmsearch.uspto.gov (last visited Oct. 10, 2019). Classes must be stylized to three digits, such that a search for Class 9 would require entering "009" as the Search Term. *Id.*

57. *Trademark Electronic Search System (TESS) Structured Search*, U.S. PAT. & TRADEMARK OFF., http://tmsearch.uspto.gov (last visited Oct. 10, 2019). I am working with a Georgetown Law student to create a tool that automates this process and generates an update when a trademark application containing "surveillance" in the goods and services description is filed.

58. *See* AMAZON RING, Registration No. 88075713, (covering, in part, "security surveillance apparatus, namely, electronic components of security systems," "software development kits (SDKs) comprising of software development tools and software for use as an application programming interface (API) for creating software and applications related to theft-prevention and security systems, and home and business surveillance systems," "electronic video surveillance products, namely, electronic components of security systems; global positioning navigation software for use with smart, autonomous vehicles and mobile machines for use in connection with internet of things (IoT) enabled devices," and "Automated self-contained electronic surveillance devices that can be deployed to gather evidence or intelligence," all in Class 9).

59. TMEP, *supra* note 36, § 904.03. All marks will eventually include a specimen, but specimens are only required for applications filed on an in-use basis. *Id.* Searching for trademark applications that include a specimen requires a Structured Search in TESS, in which the Search Term is "1A" and the Field is "Current Basis."

the application."[60] According to the Trademark Trial and Appeals Board, "[a]n important function of specimens in a trademark application is, manifestly, to enable the PTO to verify the statements made in the application regarding trademark use."[61] Effectively, specimens serve as visual demonstrations that the mark for which registration is sought is used in connection with at least one good (or service) in each class of goods or services identified in the application for registration.[62]

The type of specimen varies based on the goods or services on which the mark is used. Specimens for hardware, for example, may take the form of commercial packaging.[63] Specimens for software, however, are likely to take the form of a screenshot of the software interface or a website offering the software for sale.[64] Although the contents of specimens are not searchable using TESS, specimens for in-use applications or registered trademarks can reveal details about surveillance technologies, from the physical configuration of surveillance hardware,[65] to the features of surveillance software,[66] to the location of law enforcement customers.[67]

III. REVEALING DISCLOSURES IN TRADEMARK FILINGS FOR SURVEILLANCE TECHNOLOGIES

Revealing a surveillance technology using federal trademark filings opens new avenues for journalists, researchers, and civil society to leverage those disclosures. One may discover that a surveillance technology is in development

60. TMEP, *supra* note 36, § 904.

61. Application of Bose Corp., 546 F.2d 897 (C.C.P.A. 1976). The Federal Circuit made similar observations. *See In re* Sones, 590 F.3d 1282, 1284 (Fed. Cir. 2009) (observing that the USPTO requires specimens to ensure that applicants are using the mark in commerce).

62. TMEP, *supra* note 36, § 904.01. The TMEP offers extensive guidance about the forms that certain specimens may take. *See* TMEP, *supra* note 36, § 904. An effort to reform the process for federal trademark registration to require fewer disclosures would likely target specimens. However, specimens are a crucial piece of the registration process that ought to go unchanged, despite possible future challenges from industry.

63. TMEP, *supra* note 36, § 904.03(e).

64. *Id.*; *In re* Azteca Sys., Inc., 102 U.S.P.Q.2d 1955 (T.T.A.B. 2012). Screenshots of websites merely advertising the software are insufficient as specimens. TMEP, *supra* note 36, § 904.03(e). Similarly, displays associated with goods, including advertising and promotional materials, are not "per se 'displays' " that qualify as sufficient specimens. *See id.* § 904.03(g).

65. *See infra* Part III.A.

66. *See infra* Parts III.B–C.

67. *See, e.g.*, SHOTSPOTTER, Registration No. 3896150, Specimen (Feb. 25, 2016) (featuring a map identifying more than 50 cities across the United States, Brazil, Panama, and the United Kingdom using ShotSpotter technology, along with the years those cities began using the technology).

before there has been a public announcement.[68] One may uncover a surveillance technology whose existence has been obfuscated by non-disclosure agreements between a company and law enforcement.[69] One may find that the maker of a surveillance technology potentially exposed personal information about a target publicly.[70] Or one may unearth the terms of the financial arrangement between a company and law enforcement.[71] Each revelation presents a new opportunity to bring new information about surveillance technologies to light so that the public may play a role in deciding how these technologies are deployed—or whether they're deployed at all.

These examples form the basis of three original case studies of Harris Corporation's STINGRAY mark, Vigilant Solution's VIGILANT SOLUTIONS mark, and PredPol's PREDPOL mark. This Part explores these case studies using real trademark filings to illustrate how applications for registration of trademarks can be a source of transparency about surveillance technology, even when other transparency mechanisms fall short.

A. STINGRAY: CELL-SITE LOCATION INFORMATION INTERCEPTORS

Modern mobile phones disclose a significant amount of sensitive personal information, such as who we call, how long we talk to them, and our real-time locations. With that wealth of information at the ready, it is not surprising that law enforcement has an interest in capturing these details at the source.[72] Enter cell-site location information interceptors, or CSLI interceptors.[73] CSLI interceptors mimic cell phone communications towers in such a way that all nearby cell phones, including those of innocent passersby, are "tricked" into communicating with an interceptor rather than a cell tower operated by a telecommunications provider.[74]

68. *See, e.g.*, *supra* Part I.

69. *See infra* Part III.A.

70. *See infra* Part III.B.

71. *See infra* Part III.C.

72. Larry Greenemeier, *What Is the Big Secret Surrounding Stingray Surveillance*, SCI. AM. (June 25, 2015), https://www.scientificamerican.com/article/what-is-the-big-secret-surrounding-stingray-surveillance/.

73. For a discussion of the detailed information that can be revealed by CSLI, see Carpenter v. United States, 138 S. Ct. 2206, 2211–13 (2018). These devices are also sometimes referred to as international mobile subscriber identity, or IMSI, catchers.

74. Ryan Gallagher, *Meet the Machines That Steal Your Phone's Data*, ARS TECHNICA (Sept. 25, 2013), https://arstechnica.com/tech-policy/2013/09/meet-the-machines-that-steal-your-phones-data/.

Harris Corporation, a defense contractor based in Melbourne, Florida,[75] makes one of the most popular CSLI interceptors, sold under the brand name STINGRAY.[76] The Stingray device has become so popular in the market that "stingray" often generically refers to the whole class of technologies known as cell-site simulators.[77] Since introducing the Stingray device, Harris Corporation has taken steps to avoid transparency about its surveillance technology: Harris Corporation's website omitted any information about Stingray devices, and marketing materials came with warnings that distribution outside law enforcement or telecommunications firms could be a crime, punishable by up to five years in prison.[78] Harris Corporation petitioned the Federal Communications Commission to prevent disclosure of Stingray user manuals in response to public records requests.[79] The company even went so far as to demand that law enforcement using Stingray devices agree and adhere to strict

75. *Locations*, HARRIS CORP., https://www.harris.com/locations (last visited Mar. 20, 2018) (noting the location of their corporate headquarters).

76. STINGRAY, Registration No. 2762468 (Sept. 9, 2003). Harris Corporation makes many other pieces of surveillance technology, including DENALI, Registration No. 5628200 (filed Dec. 11, 2018) (Class 9 covering, in part, "firmware installable in communications transceivers for enabling such transceivers to encrypt and decrypt information communicated via the transceivers"), and KINGFISH, Registration No. 2867227 (July 27, 2004) (Class 9 covering "electronic surveillance transceivers for tracking, locating and gathering information from cellular telephones").

77. *See, e.g.*, Jennifer Valentino-DeVries, "*Stingray" Phone Tracker Fuels Constitutional Clash*, WALL ST. J. (Sept. 22, 2011), https://www.wsj.com/articles/SB10001424053111904194604576583112723197574; Gallagher, *supra* note 74 (noting that the term "stingray" is used generically). The terms "cell site location information interceptors" and "cell-site simulators" are used interchangeably.

78. Gallagher, *supra* note 74.

79. Letter from Tania W. Hanna, Vice President of Government Relations, Harris Corp., to Julius P. Knapp, Chief of Office of Engineering and Technology, FCC, Request for Confidentiality of Harris Corporation for FCC ID Nos. NK73092523, NK73100176, NK73166210 (Oct. 20, 2014), https://www.scribd.com/document/259988405/Harris-Letter-Response-Request-for-Confidentiality-FOIA-2014-669; Matthew Keys, *Exclusive: StingRayMaker Asked FCC To Block Release of Spy Gear Manual*, THE BLOT (Mar. 26, 2015), https://www.theblot.com/exclusive-stingray-maker-asked-fcc-to-block-release-of-spy-gear-manual-7739514; *see also* Nathan Freed Wessler & Nicole Ozer, *Documents Suggest Maker of Controversial Surveillance Tool Misled the FCC*, ACLU: FREE FUTURE (Sept. 17, 2014), https://www.aclu.org/blog/documents-suggest-maker-controversial-surveillance-tool-misled-fcc?redirect=blog/national-security/documents-suggest-maker-controversial-surveillance-tool-misled-fcc (observing that Harris claimed that its Stingray technology would only be used for emergencies despite records released by the Tallahassee, Florida Police Department suggesting that only 29% of cases involving a Stingray were "emergencies").

non-disclosure agreements prohibiting those agencies from disclosing any details about Harris' equipment, including its existence—even to judges.[80]

Perhaps Harris Corporation's dedication to avoiding transparency explains why it took some time for the public to receive its first federal case to mention Stingray devices.[81] In *United States v. Allums*, the defendant, James Edward Allums, was charged with three robberies, in part based on the CSLI of Allums' cell phone.[82] As Judge Stewart explained, the government used a phone and "another device called a Stingray, which also tracked which cell tower was the strongest at any geographical position," to identify the location of Allums.[83] The unpublished memorandum decision was released in 2009, but it took until 2014 for the American Civil Liberties Union to use a public records request to obtain emails (also written in 2009) revealing that law enforcement in Florida had been misleading judges, defense counsel, and defendants about the use of Stingray devices.[84]

---

80. *See, e.g.*, Thomas v. State, 127 So.3d 658, 660 (Fla. Dist. Ct. App. 2013) (noting that local police department "did not want to obtain a search warrant because they did not want to reveal information about the technology they used to track the cell phone signal" due to a non-disclosure agreement with Harris Corporation); *see also* Kim Zetter, *Police Contract with Spy Tool Maker Prohibits Talking About Device's Use*, WIRED (Mar. 4, 2014), https://www.wired.com/2014/03/harris-stingray-nda/ (providing an example of an NDA attached to the use of police surveillance equipment); Spencer McCandless, Note, *Stingray Confidential*, 85 GEO. WASH. L. REV. 993 (2017), http://www.gwlr.org/wp-content/uploads/2017/07/85-Geo.-Wash.-L.-Rev.-993.pdf (considering the long history of the use of "stingray" devices and the secrecy surrounding them).

81. United States v. Allums, No. 2:08-CR-30 TS (D. Utah, Mar. 24, 2009). The *Rigmaiden* case, which involved a pro se defendant who successfully demonstrated that a warrantless cell-site location information interceptor was used to investigate his case, is often identified as the first case to publicly reveal the existence of Stingray devices—but the final decision, which discussed Stingray devices, was not decided until 2013. *See* United States v. Rigmaiden, No. CR 08-814-PHX-DGC (D. Ariz. May. 8, 2013). That said, similar devices were in use well before 2009—the Harris Corporation's Triggerfish device was promoted as early as 1991. *See* Stephanie K. Pell & Christopher Soghoian, *A Lot More Than a Pen Register, and Less Than a Wiretap: What the Stingray Teaches Us About How Congress Should Approach the Reform of Law Enforcement Surveillance Authorities*, 16 YALE J. L. & TECH. 134, 142 (2014) ; *see also* Tsutomu Shimomura, *Catching Kevin*, WIRED (Feb. 1, 1996), https://www.wired.com/1996/02/catching/ (describing how a cell-site simulator was used to track hacker Kevin Mitnick, along with a Triggerfish device). The earliest trademark application for the TRIGGERFISH mark was filed in 2001. *See* TRIGGERFISH, Registration No. 2534253 (Jan. 29, 2002)(cancelled Oct. 31, 2008).

82. *Allums*, No. 2:08-CR-30 TS at 1.

83. *Id.* at 2.

84. Maria Kayanan, *Internal Police Emails Show Efforts to Hide Use of Cell Phone Tracking*, ACLU: FREE FUTURE (June 19, 2014), https://www.aclu.org/blog/national-security/privacy-and-surveillance/internal-police-emails-show-efforts-hide-use-cell?redirect=blog/national-security-technology-and-liberty/internal-police-emails-show-efforts-hide-use-cell.

If someone had been scanning federal trademark filings, however, the public would have known about the existence of Stingray devices nearly a decade sooner.[85] On August 21, 2001, Harris Corporation filed a federal trademark application for the STINGRAY mark.[86] The mark was filed with an intent-to-use designation, with the first use date of March 2, 2003.[87] As registered, the mark covers "multi-channel, software-defined, two-way electronic surveillance radios for authorized law enforcement agencies for interrogating, locating, tracking and gathering information from cellular telephones" in Class 9.[88] The specimen depicts an actual Stingray device, emblazed with the logo, and depicting the inputs and outputs embedded in the device.[89]

Using federal trademark filings, the public could have learned about the existence of CSLI interceptors nearly a decade before the first federal court decision disclosing the existence of Stingray devices.

85. Harris Corporation also patented the Stingray device even earlier than filing its trademark application. U.S. Patent No. 5428667A (June 27, 1995), https://patents.google.com/patent/US5428667A/en.

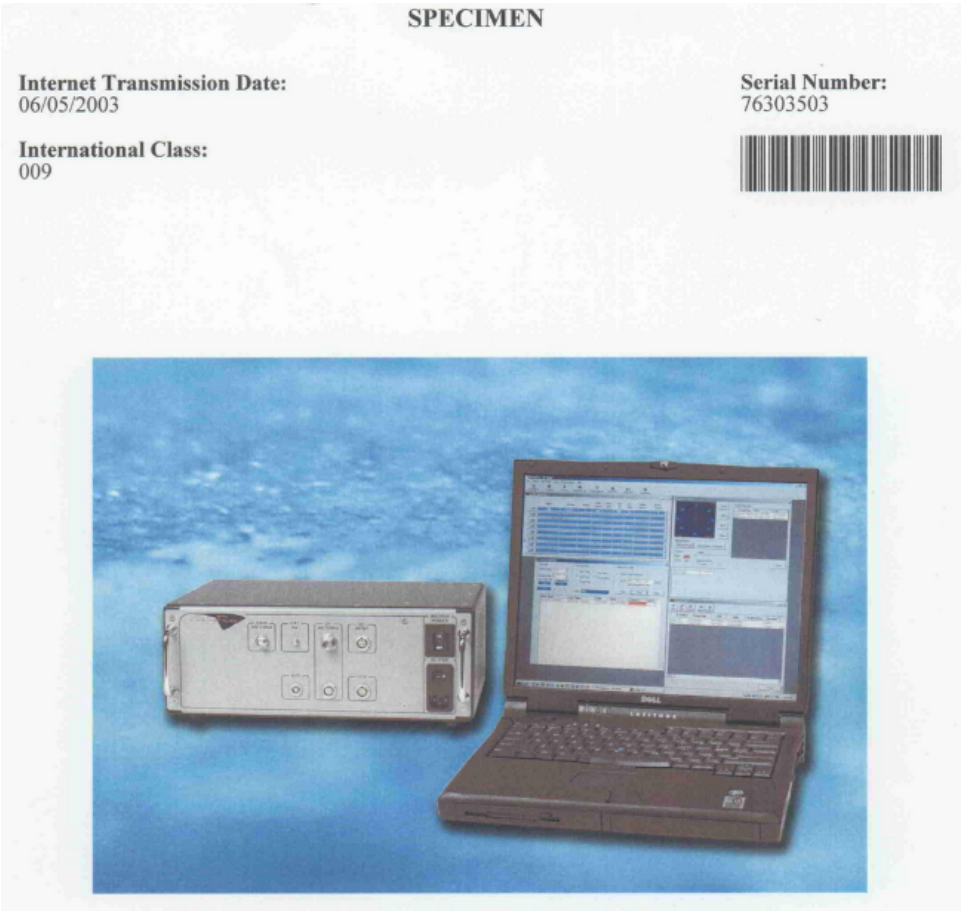
86. STINGRAY, Registration No. 2762468 (Sept. 9, 2003).

87. *Id.*

88. *Id.*

89. STINGRAY, Registration No. 2762468, Specimen (June 18, 2003). The specimen was the second specimen submitted; the prior specimen borders on illegible due to the quality of the images included. *See* STINGRAY, Registration No. 2762468 (June 5, 2003).

Figure 1: Stingray CSLI Interceptor



B. VIGILANT SOLUTIONS: AUTOMATED LICENSE PLATE READERS

Certain private corporations regularly take photographs of cars, trucks, and other automobiles and sell those images to law enforcement. These companies mount small high-speed cameras called automated license plate readers, or ALPRs, on moving police vehicles or stationary infrastructure like bridges or

roads,[90] which then photograph up to thousands of license plates per minute.[91] The photographs are then stored in searchable databases used by law enforcement.[92] According to the International Association of Chiefs of Police, law enforcement agencies can use ALPRs to "enhance their enforcement and investigative capabilities, expand their collection of relevant data, and expedite the tedious and time consuming [sic] process of comparing vehicle license plates with lists of stolen, wanted, and other vehicles of interest."[93] ALPRs also enable surveillance by empowering law enforcement to track a single vehicle across cities and states with no suspicion of wrongdoing—a task that would be challenging, if not impossible, for someone peeking out of a window and jotting down license plate numbers.[94]

ALPR databases are also abused blatantly.[95] In 2016, for example, a Washington D.C. police officer pleaded guilty to extortion after blackmailing car owners whose vehicles were identified near a gay bar.[96] The year before, a SWAT team mistakenly raided a man's house searching for a marijuana-growing operation because of license plate monitoring at a garden store but found no evidence of such an operation.[97] And several years before that, police

90. Ellen Nakashima & Josh Hicks, *Homeland Security is Seeking a National License Plate Tracking System*, WASH. POST (Feb. 18, 2014), https://www.washingtonpost.com/world/national-security/homeland-security-is-seeking-a-national-license-plate-tracking-system/2014/02/18/56474ae8-9816-11e3-9616-d367fa6ea99b_story.html?noredirect=on&utm_term=.876d14309e14.

91. *Automatic License Plate Readers*, AM. CIV. LIBERTIES UNION, https://www.aclu.org/issues/privacy-technology/location-tracking/automatic-license-plate-readers (last visited Mar. 20, 2018).

92. *See generally Vigilant Platesearch™*, VIGILANT SOLUTIONS, https://www.vigilantsolutions.com/products/license-plate-recognition-lpr/ (last visited Feb. 22, 2020).

93. *Automated License Plate Recognition*, INT'L ASS'N OF CHIEFS OF POLICE, https://www.theiacp.org/projects/automated-license-plate-recognition (last visited Mar. 20, 2018).

94. For a comprehensive exploration of local law enforcement use of ALPRs and the transparency challenges posed by those relationships, see generally Bryce Clayton Newell, *Local Law Enforcement Jumps on the Big Data Bandwagon: Automated License Plate Recognition Systems, Information Privacy, and Access to Government Information*, 66 MAINE L. REV. 398 (2014), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2341182.

95. Julia Angwin & Jennifer Valentino-DeVries, *New Tracking Frontier: Your License Plates*, WALL ST. J. (Sept. 29, 2012), https://www.wsj.com/articles/SB10000872396390443995604578004723603576296.

96. Anthony D. Romero, *Documents Uncover NYPD's Vast License Plate Reader Database*, HUFFINGTON POST (Jan. 26, 2016), https://www.huffingtonpost.com/mariko-hirose-/documents-uncover-nypds-v_b_9070270.html; *see also* Mariko Hirose, *Documents Uncover NYPD's Vast License Plate Reader Database*, ACLU: FREE FUTURE (Jan. 25, 2016), https://www.aclu.org/blog/privacy-technology/location-tracking/documents-uncover-nypds-vast-license-plate-reader-database.

97. Radley Balko, *Federal Judge: Drinking Tea, Shopping at a Gardening Store is Probable Cause for a SWAT Raid on Your Home*, WASH. POST (Dec. 28, 2015), https://

removed a woman from her car at gunpoint on the mistaken belief that she was driving a stolen car after a license plate reader had misread her plates.[98]

Most states do not regulate ALPRs.[99] But sixteen states, including California, Florida, and Maryland, do have laws regarding license plate readers and data retention.[100] These laws can still be insufficient to deter misconduct. In early 2020, a California auditor discovered widespread issues with use of license plate readers across in the state, from insecurely storing data to sharing images with thousands of entities across the United States without determining whether those entities had a right or need to access the images.[101]

One of the leading ALPR vendors is Vigilant Solutions, a company based in Livermore, California.[102] Vigilant Solutions takes information that can be unwieldy to manage and collect—like photographs of license plates—and assembles that information into databases for private clients.[103] In its marketing materials, Vigilant Solutions advertises that its license plate recognition tools scan photographs of license plates along with the date, time, and location of where a particular vehicle was photographed.[104] Chris Metaxas, a chief

---

www.washingtonpost.com/news/the-watch/wp/2015/12/28/federal-judge-drinking-tea-shopping-at-a-gardening-store-is-probable-cause-for-a-swat-raid-on-your-home/?utm_term=.44d1bc082ee9; Romero, *supra* note 96.

98. Kade Crockford, *San Francisco Woman Pulled Out of Car at Gunpoint Because of License Plate Reader Error*, ACLU: FREE FUTURE (May 13, 2014), https://www.aclu.org/blog/privacy-technology/location-tracking/san-francisco-woman-pulled-out-car-gunpoint-because.

99. *Automated License Plate Readers: State Statutes*, NAT'L CONF. OF STATE LEGISLATURES, http://www.ncsl.org/research/telecommunications-and-information-technology/state-statutes-regulating-the-use-of-automated-license-plate-readers-alpr-or-alpr-data.aspx (updated Oct. 23, 2020).

100. *Id.* Arkansas, Colorado, Georgia, Maine, Minnesota, Montana, Nebraska, New Hampshire, North Carolina, Oklahoma, Tennessee, and Utah also have ALPR laws. *Id.* Vermont repealed its ALPR law in 2020. *See Vermont Statutes Online*, VT. GEN. ASSEMBLY, https://legislature.vermont.gov/statutes/section/23/015/01607 (last visited Nov. 19, 2020).

101. ELAINE M. HOWLE, CALIFORNIA STATE AUDITOR, REPORT NO. 2019-118: SUMMARY OF AUTOMATED LICENSE PLATE READERS: TO BETTER PROTECT INDIVIDUALS' PRIVACY, LAW ENFORCEMENT MUST INCREASE ITS SAFEGUARDS FOR THE DATA IT COLLECTS (2020), https://www.auditor.ca.gov/reports/2019-118/index.html.

102. *Our Passion*, VIGILANT SOLUTIONS, https://www.vigilantsolutions.com/our-passion/ (last visited Nov. 17, 2020). Based on its website, Vigilant Solutions is expanding into facial recognition technology. *See Vigilant Facesearch™*, VIGILANT SOLUTIONS, https://www.vigilantsolutions.com/products/facial-recognition/ (last visited Oct. 28, 2019).

103. Dan Froomkin, *Reports of the Death of a National License-Plate Tracking Database Have Been Greatly Exaggerated*, THE INTERCEPT (Mar. 17, 2014), https://theintercept.com/2014/03/17/1756license-plate-tracking-database/ (detailing the national network of license plate databases).

104. *Vigilant Solutions, PlateSearch*, VIGILANT SOLUTIONS, https:// www.motorolasolutions.com/content/dam/msi/docs/products/license-plate-recognition-systems/reaperhd-mobile-lpr-system/vigilant_platesearch_fact_sheet.pdf (last visited Aug. 8, 2021).

executive for Vigilant Solutions' subsidiary DRN, compared the company's work to "a guy holding his head out the window, looking down the block, and writing license-plate numbers down and comparing them against a list. The technology just makes things better and more productive."[105] Vigilant Solutions' technology certainly makes surveillance easier: Vigilant Solutions advertises that its commercial dataset offers more than 5 billion license plate detections, with more than 150 million plates added each month.[106]

Discovering information about ALPRs can be challenging. In 2018, the Electronic Frontier Foundation (EFF) used public records requests to find out more information about the procurement and deployment of ALPRs. EFF partnered with Muckrock—a nonprofit organization dedicated to public records requests—to file a series of requests to gather details about more than 200 cities' ALPR programs.[107] Responses to these requests revealed that fewer than 1% of the 2.5 billion license plates scanned in the years 2016 and 2017 were linked to cars under any suspicion at the time the plates were captured.[108] EFF concluded that law enforcement agencies shared their data with a minimum of 160 other agencies, all through Vigilant Solutions' LEARN program, an acronym for Law Enforcement Archival and Reporting Network.[109] In response to EFF and MuckRock's FOIA requests, Vigilant Solutions reached out to at least one jurisdiction to assure the city that "quite simply…we are here for you."[110]

105. Nakashima & Hicks, *supra* note 90.

106. *Vigilant Solutions*, MOBILCOMM (last visited Nov. 18, 2020), https://www.mobilcomm.com/vigilant-solutions/; *see also* Gwyndolyn Wu, *ICE Had Access to Hundreds of Millions of License Plates*, S.F. CHRON. (Mar. 13, 2019), https://www.sfchronicle.com/crime/article/ICE-had-access-to-hundreds-of-millions-of-license-13685652.php.

107. David Maass & Beryl Lipton, *EFF and MuckRock Release Records and Data from 200 Law Enforcement Agencies' Automated License Plate Reader Programs*, EFF DEEPLINKS (Nov. 15, 2018), https://www.eff.org/deeplinks/2018/11/eff-and-muckrock-release-records-and-data-200-law-enforcement-agencies-automated; *see also* Cory Doctorow, *Here's the Secret Details of 200 Cities' License-Plate Tracking Programs*, BOINGBOING (Nov. 15, 2018), https://boingboing.net/2018/11/15/find-yourself-a-city-to-live-i.html.

108. Dave Maass & Beryl Lipton, *Data Driven: Explore How Cops Are Collecting and Sharing Our Travel Patterns Using Automated License Plate Readers*, EFF, https://www.eff.org/pages/automated-license-plate-reader-dataset (last visited Nov. 19. 2020).

109. *Id.* Vigilant Solutions has been unimpressed by EFF's investigations into its technology and policies. *See, e.g.*, Susan Crandall, *EFF: Stop Creating Fake News and Scaring People!*, VIGILANT SOLUTIONS (July 12, 2018), https://www.vigilantsolutions.com/eff-stop-creating-fake-news-scaring-people/ (responding to an EFF investigation that linked a Vigilant Solutions customer that manages several California malls to vehicle data shared with Immigration and Customs Enforcement (ICE)).

110. Camille Fassett, *License Plate Surveillance Company Attacks Nonprofits for Filing FOIA Requests*, VICE (Apr. 4, 2018), https://www.vice.com/en/article/3kjp85/vigilant-solutions-eff-muckrock-foia-requests.

Vigilant Solutions has two federally registered trademarks. One is a design mark for a three-part disjointed V with the words VIGILANT SOLUTIONS stacked on top of one another to the right of the V, was filed on June 26, 2014.[111] The VIGILANT SOLUTIONS design mark covers "computer hardware and software in the fields of law enforcement and crime prevention for identifying human faces and vehicle license plates, for tracking vehicles over time and geographic location, and for producing reports on the movements of specific vehicles" in Class 9.[112]

But it is the VIGILANT SOLUTIONS specimen that is especially revealing—it features what appears to be authentic geolocation data linked to real license plate numbers:

Figure 2: Vigilant Solutions LEARN Interface

Applicant: Vigilant Solutions, Inc.

Mark: VIGILANT SOLUTIONS & V Design

111. VIGILANT SOLUTIONS, Registration No. 4780381 (July 28, 2015).
112. *Id.*

Vigilant Solutions appears to have submitted an image from its LEARN database depicting four license plate numbers, all of which are clearly legible in the specimen.[113] The specimen also appears to reveal the precise latitude and longitude data for a specific license plate number.[114] According to the specimen, the plate was identified through private data and a private system on Dam Neck Road in Virginia Beach, Virginia.[115] The specimen includes a visualization of the location.[116]

The other, earlier registration is for the image of a disjointed V, filed on August 13, 2013.[117] The mark covers "[c]omputer hardware and software in the fields of security and law enforcement for tracking vehicles over time and geographic location and for producing reports on the movements of specific vehicles" in Class 9.[118]

The specimen appears to show an interface for a "Vigilant Stakeout—Report" and depicts an exact address in Homestead, Florida.[119] Visit number 21 is highlighted with 531 plates scanned, but the target plate does not appear to have been scanned.[120] The bottom of the specimen features five images of car bumpers, each featuring their respective license plate numbers, as well as the date and time the cars were scanned.[121]

113. VIGILANT SOLUTIONS, Registration No. 4780381, Specimen (June 26, 2014).
114. *Id.*
115. *Id.*
116. *Id.*
117. VIGILANT SOLUTIONS, Registration No. 4528520 (May 13, 2014).
118. *Id.*
119. VIGILANT SOLUTIONS, Registration No. 4528520, Specimen (Aug. 13, 2013).
120. *Id.*
121. *Id.*

Figure 3: Vigilant Solutions LEARN Interface

Applicant: Vigilant Solutions, Inc.

Mark: VIGILANT SOLUTIONS & V Design

Vigilant Solutions' trademark filings offer an additional approach to surveillance transparency, in which the public reveals that a company may have failed to protect the sensitive information that it collects.[122] There has already been backlash to the deployment of ALPRs in communities without public approval,[123] and these specimens may further fuel transparency by offering journalists and civil liberties organizations an alarming new talking point.

C. PREDPOL: PREDICTIVE POLICING ALGORITHMS

Predictive policing uses algorithms that attempt to predict the geographical locations of future crimes using data drawn from past crime statistics and other

122. *See supra* note 119.

123. It's worth noting that some reports suggest that surveillance cameras, like those that fuel ALPR systems, do not have a measurable impact on reducing crime. *See, e.g.*, Sonia Roubini, *Police Chief: Surveillance Cameras Don't Help Fight Crime*, ACLU: FREE FUTURE (Apr. 9, 2015), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/police-chief-surveillance-cameras-dont-help-fight.

information.[124] The company PredPol describes itself as the market leader in predictive policing technology.[125] The "past crime statistics and other information" used by PredPol's algorithm include victimization data, meaning crimes that have been reported to law enforcement.[126]

PredPol is not without controversy. Relying on crime data that reflects systemic racial bias as training data—dubbed "dirty data" by Rashida Richardson, Kate Crawford, and Jason Schultz—can effectively amplify those biases.[127] PredPol remains a private company, developed from research conducted by the University of California, Los Angeles and the Los Angeles Police Department,[128] but only individuals who have financial interests in PredPol have conducted research on the company's methodology.[129] Some of those jurisdictions, like the Los Angeles Police Department, have been candid and forthcoming about their use of PredPol algorithms to evaluate crimes.[130]

Others have been far less transparent, leading researchers to resort to clever techniques to try to learn more about PredPol's partnerships and practices. In 2018, a security researcher used a series of domain-name logins to identify a dozen cities with previously undisclosed relationships with PredPol.[131] Journalist Caroline Haskins used the domain names as a starting

124. Andrew Guthrie Ferguson, *Predictive Policing and Reasonable Suspicion*, 62 EMORY L.J. 259 (2012). For a comprehensive accounting of attempts to bring oversight to predictive policing technologies, see generally FERGUSON, THE RISE OF BIG DATA POLICING (2017) and Andrew G. Ferguson, *Policing Predictive Policing*, 94 WASH. U. L. REV. 1109 (2017) (hereinafter *Policing Predictive Policing*).

125. *Overview*, PREDPOL, https://www.predpol.com/about/ (last visited Mar. 18, 2019).

126. *Id.* As Ferguson notes, "PredPol's primary business of targeting burglary and auto-related crimes avoids many of the data collection problems of a broader crime focus." *Policing Predictive Policing*, *supra* note 124, at 1148.

127. Rashida Richardson, Kate Crawford & Jason Schultz, *Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice*, N.Y.U. L. REV. ONLINE (forthcoming). For a discussion of implicit bias becoming embedded in artificial intelligence systems, see generally Amanda Levendowski, *How Copyright Law Can Fix Artificial Intelligence's Implicit Bias Problem*, 93 WASH. L. REV. 579 (2018).

128. PREDPOL, *supra* note 125; *see also* Robert Brauneis & Ellen P. Goodman, *Algorithmic Transparency for the Smart City*, 20 YALE J. L. & TECH. 103, 146 (2018).

129. Emily Berman, *A Government of Laws and Not of Machines*, 98 BOSTON U. L. REV. 1277, 1307 (2018) (citing Darwin Bond Graham, *Oakland Mayor Schaaf and Police Seek Unproven "Predictive Policing" Software*, EAST BAY EXPRESS (June 24, 2015), https://www.eastbay express.com/oakland/oakland-mayor-schaaf-and-police-seek-unproven-predictive-policing-software/Content?oid=4362343).

130. *See* Ferguson, *supra* note 124, at 261; *see also* Leila Miller, *LAPD Will End Controversial Program that Predicts Where Crimes Would Occur*, L.A. TIMES (Apr. 21, 2020), https:// www.latimes.com/california/story/2020-04-21/lapd-ends-predictive-policing-program.

131. Cory Doctorow, *Is This the Full List of US Cities That Have Bought Or Considered PredPol's Predictive Policing Services?*, BOINGBOING (Oct. 30, 2018), https://boingboing.net/2018/10/30/ el-monte-and-tacoma.html.

point for her own series of public record requests for PredPol contracts and negotiation emails, instruction manuals, and slide presentations.[132] That same year, researchers Ellen Goodman and Robert Brauneis sent public records requests to eleven police departments, eight of which declined to respond or acknowledged the request without producing any responsive documents.[133] One city even stated that "[t]he City Attorney has advised that information revealing surveillance techniques, procedures or personnel is exempt from public inspection pursuant to s. 119.071(2)(d), Florida statutes."[134]

Neither investigation revealed a relationship between PredPol and the city of Richmond, California, a small city in the East Bay.[135] The existence of Richmond's contract with PredPol was not exactly a secret,[136] but the details were revealed somewhere surprising: federal trademark filings.[137] PredPol filed a trademark application for the PREDPOL mark on February 2, 2012 covering, in part, "computer software for use in law enforcement and related business, namely, computer software used for use in the analysis and determination of probable locations where crimes will be committed with information delivery through browser and portable device applications and map overlays" in Class 9.[138]

132. Caroline Haskins, *Dozens of Cities Have Secretly Experimented with Predictive Policing Softwar*e, MOTHERBOARD, Feb. 6, 2019, https://www.vice.com/en/article/d3m7jq/dozens-of-cities-have-secretly-experimented-with-predictive-policing-software.

133. Brauneis & Goodman, *supra* note 128, at 146–47.

134. *Id.* at 147 (quoting Legislation Details (With Text), CITY OF COCOA, FILE # 15-361, (July 30, 2015), http://cdn.muckrock.com/foia_files/2017/01/13/15-361_City_Council_Agenda_Item__8-25-15.pdf).

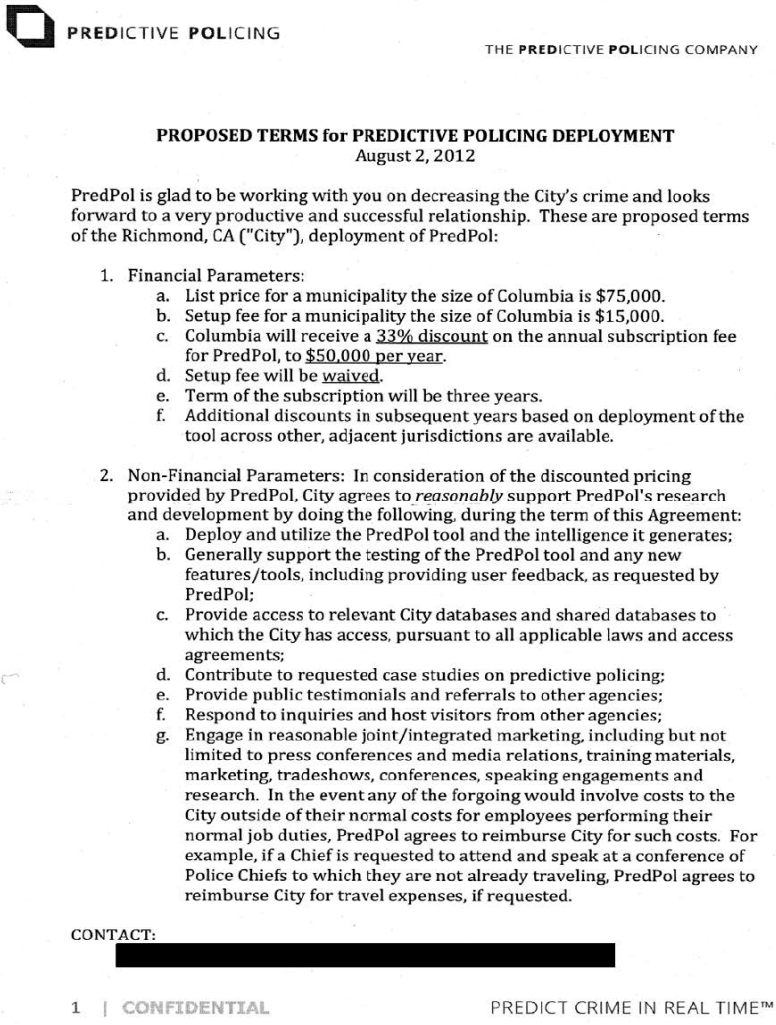
135. *Richmond, California*, WIKIPEDIA, https://en.wikipedia.org/wiki/Richmond,_California (last visited Mar. 18, 2018).

136. *SF Weekly* reported that Richmond was using PredPol technology in 2013. Darwin Bond-Graham, *All Tomorrow's Crimes: The Future of Policing Looks a Lot Like Good Branding*, SF WEEKLY (Oct. 30, 2013), http://www.sfweekly.com/news/all-tomorrows-crimes-the-future-of-policing-looks-a-lot-like-good-branding/. The *East Bay Express* published a critical follow up several years later. *See* Bond-Graham, *supra* note 129. Unlike some acquisitions of surveillance technologies, Oakland Mayor Libby Schaaf disclosed the contract with PredPol in her 2015-2017 budget for the city. *Id.*

137. PREDPOL, Registration No. 4299222 (Mar. 5, 2013).

138. *Id.*

Figure 4: PredPol Contract



PREDICTIVE POLICING

THE PREDICTIVE POLICING COMPANY

PROPOSED TERMS for PREDICTIVE POLICING DEPLOYMENT
August 2, 2012

PredPol is glad to be working with you on decreasing the City's crime and looks forward to a very productive and successful relationship. These are proposed terms of the Richmond, CA ("City"), deployment of PredPol:

1. Financial Parameters:
   a. List price for a municipality the size of Columbia is $75,000.
   b. Setup fee for a municipality the size of Columbia is $15,000.
   c. Columbia will receive a 33% discount on the annual subscription fee for PredPol, to $50,000 per year.
   d. Setup fee will be waived.
   e. Term of the subscription will be three years.
   f. Additional discounts in subsequent years based on deployment of the tool across other, adjacent jurisdictions are available.

2. Non-Financial Parameters: In consideration of the discounted pricing provided by PredPol, City agrees to *reasonably* support PredPol's research and development by doing the following, during the term of this Agreement:
   a. Deploy and utilize the PredPol tool and the intelligence it generates;
   b. Generally support the testing of the PredPol tool and any new features/tools, including providing user feedback, as requested by PredPol;
   c. Provide access to relevant City databases and shared databases to which the City has access, pursuant to all applicable laws and access agreements;
   d. Contribute to requested case studies on predictive policing;
   e. Provide public testimonials and referrals to other agencies;
   f. Respond to inquiries and host visitors from other agencies;
   g. Engage in reasonable joint/integrated marketing, including but not limited to press conferences and media relations, training materials, marketing, tradeshows, conferences, speaking engagements and research. In the event any of the forgoing would involve costs to the City outside of their normal costs for employees performing their normal job duties, PredPol agrees to reimburse City for such costs. For example, if a Chief is requested to attend and speak at a conference of Police Chiefs to which they are not already traveling, PredPol agrees to reimburse City for travel expenses, if requested.

CONTACT: [redacted]

1 | CONFIDENTIAL PREDICT CRIME IN REAL TIME™

On December 13, 2012, PredPol submitted a specimen showing the PREDPOL mark as used in commerce.[139] The majority of the specimen appears to be marketing materials explaining the mechanics of how PredPol

139. PREDPOL, Registration No. 4299222, Specimen (Dec. 13, 2012). The specimen has been lightly redacted, as the original specimen uploaded by PredPol reveals the cell phone number of someone who appears to be an employee.

works and the ways in which it can benefit law enforcement.[140] But, beginning on the third page, PredPol submitted a contract that lays out the proposed terms for a PREDPOL software deployment for the city of "Richmond, CA."[141] The contract begins by explaining that "PredPol is glad to be working with you on decreasing the City's crime and looks forward to a very productive and successful relationship."[142]

The contract is dated August 2, 2012,[143] and it identifies the financial parameters for the agreement. It states that the "list price for a municipality the size of Columbia is $75,000" and the "setup fee is…$15,000."[144] The contract appears to provide Richmond with two discounts: "Columbia [*sic*] will receive a 33% discount on the annual subscription fee for PredPol, to $50,000 per year" and the "[s]etup fee will be waived."[145] The term of the subscription is three years.[146] There is also a provision providing that "[a]dditional discounts in subsequent years based on deployment of the tool across other, adjacent jurisdictions are available."[147]

The most shocking term of the contract is Richmond's agreement to support PredPol and its work in exchange for the discounted pricing.[148] The contract states that "City agrees to *reasonably* support PredPol's research and development by doing the following, during the term of this Agreement…[p]rovide public testimonials and referrals to other agencies" and "[e]ngage in reasonable joint/integrated marketing, including but not limited to press conferences and media relations, training materials, marketing, tradeshows, conferences, speaking engagements and research."[149] If any of the previously mentioned support would "involve costs to the City outside of their normal costs for employees performing their normal job duties, PredPol agrees to reimburse City for such costs. For example, if a Chief is requested to attend and speak at a conference of Police Chiefs to which they are not already traveling, PredPol agrees to reimburse City for travel expenses, if requested."[150] The document is marked "CONFIDENTIAL" at the bottom.[151]

140. *Id.*
141. *Id.*
142. *Id.*
143. *Id.*
144. *Id.* The city of Columbia is referenced at several points in the contract. It is not clear why one reference is comparative and the other appears to be a mistake in the contract.
145. PREDPOL, Registration No. 4299222, Specimen (Dec. 13, 2012).
146. *Id.*
147. *Id.*
148. *See id.*
149. *Id.*
150. *Id.*
151. *Id.*

Despite its apparent contractual agreement to support PredPol, the Richmond Police Department terminated its relationship with the company in 2016, midway through a multi-year contract, because the city found that there was no measurable impact on crime reduction.[152] It does not yet appear that journalists and civil liberties organizations have filed public records requests to determine whether Richmond received any additional discounts on its PredPol contract or took advantage of PredPol's offer to reimburse travel expenses in exchange for "reasonably supporting" PredPol's research and development.

IV. CONCLUSION

If the public had known the details about the secret surveillance technologies tricking our cell phones, tracking our license plates, and telegraphing our prospective criminality, perhaps we could have refused these technologies' use before they became firmly rooted in our criminal legal system. Surveillance transparency is tricky, but we need it more than ever. How can we resist invasive surveillance technologies, created by corporations and embraced by law enforcement, when we are not aware of the threats? Using federal trademark filings to investigate existing and future surveillance technologies offers journalists, researchers, and civil society the opportunity to better understand dangerous surveillance technologies and, hopefully, energize the public to mount a resistance.[153] By using federal trademark filings for surveillance transparency, we can adopt one more way to resist an entrenched power dynamic: the watched can become watchers.

152. Emily Thomas, *Why Oakland Police Turned Down Predictive Policing*, MOTHERBOARD (Dec. 28, 2016), https://motherboard.vice.com/en_us/article/ezp8zp/minority-retort-why-oakland-police-turned-down-predictive-policing; David Robinson & Logan Koepke, *Stuck in a Pattern: Early Evidence on "Predictive Policing" and Civil Rights*, UPTURN (Aug. 2016), https://www.upturn.org/reports/2016/stuck-in-a-pattern/.

153. The author hopes that the public will also embrace tools that scan the USPTO database for new trademark filings for surveillance technology.