



Summer 6-1-2015

Spying Inc.

Danielle Keats Citron
University of Maryland School of Law

Follow this and additional works at: <https://scholarlycommons.law.wlu.edu/wlulr>



Part of the [Privacy Law Commons](#)

Recommended Citation

Danielle Keats Citron, *Spying Inc.*, 72 Wash. & Lee L. Rev. 1243 (2015).

Available at: <https://scholarlycommons.law.wlu.edu/wlulr/vol72/iss3/7>

This Article is brought to you for free and open access by the Washington and Lee Law Review at Washington and Lee University School of Law Scholarly Commons. It has been accepted for inclusion in Washington and Lee Law Review by an authorized editor of Washington and Lee University School of Law Scholarly Commons. For more information, please contact christensena@wlu.edu.

Spying Inc.

Danielle Keats Citron*

Abstract

The latest spying craze is the “stalking app.” Once installed on someone’s cell phone, the stalking app can provide continuous access to the phone owner’s calls, texts, snapchats, photos, calendar updates, and movements. Stalking apps destroy the privacy and confidentiality of cell phone activities. Domestic abusers and stalkers frequently turn to stalking apps because they are undetectable even to sophisticated phone owners.

Business is booming for stalking app providers, even though their entire enterprise is arguably illegal. Federal and state wiretapping laws ban the manufacture, sale, or advertisement of devices knowing their design makes them primarily useful for the surreptitious interception of electronic communications. But those laws are rarely, if ever, enforced. Existing law may be too restrictive to make a real difference.

A legal agenda is essential to combating the growth of stalking software. We need to update criminal and civil penalties facing providers. Record-keeping requirements could help decrease the demand for spyware. Private rights of action, if recognized, could

* Danielle Keats Citron, Lois K. Macht Research Professor & Professor of Law, University of Maryland Francis King Carey School of Law, Affiliate Fellow, Yale Information Society Project, Affiliate Scholar, Stanford Center on Internet and Society. Serious thanks to Alvaro Bedoya, Angela Campbell, Bobby Chesney, Julie Cohen, Leslie Henry, David Gray, Josh Fairfield, Nathaniel Gleicher, Woodrow Hartzog, Margaret Hu, Robert Mosbacher, Chris Slobogin, Rachel Levinson-Waldman, Craig Timber, and David Vladeck for their insights. Jeffrey Rabkin kindly read drafts with his expert eye. Venus Johnson, Robert Morgester, and the rest of Attorney General Kamala Harris’s Task Force on Cyber Exploitation offered suggestions. Thanks as well to the Georgetown-Maryland Privacy Working Group. I am grateful to the National Network to End Domestic Violence, most especially Cindy Southworth, for their help and crucial advocacy. Cassie Mejias, Frank Lancaster, and Mariel Shutinya helped me with research. Susan McCarty, as always, was a superb reader, editor, and footnote fixer. The suggestions of the participants in the Washington & Lee Law Review’s Cybersurveillance in the Post-Snowden Age symposium were superb; Paul Wiley, Kelton Frye, and their team of editors were a huge help.

help secure redress and deterrence. To increase the likelihood that the law will be enforced, states and localities need more training and digital forensic expertise. The private sector could reinforce these efforts by offering devices that can resist the installation of spyware.

Table of Contents

| | |
|---|------|
| I. Introduction | 1244 |
| II. The Private Surveillance Business | 1253 |
| A. Evolution of the Spying Trade..... | 1253 |
| B. Private Spying 2.0 | 1255 |
| C. Perils of Spyware | 1257 |
| III. Law's Role Combating Spying Inc..... | 1259 |
| A. Historical Development of Wiretapping Laws | 1259 |
| B. Cutting Off the Source: Section 2512 and Analogous State Statutes | 1263 |
| C. Consumer Protection Laws | 1269 |
| IV. Next Steps..... | 1273 |
| A. Updating the Law | 1274 |
| B. Enforcement Efforts | 1279 |
| C. Private Sector Solutions | 1279 |
| V. Conclusion..... | 1280 |
| VI. Appendix | 1281 |

I. Introduction

Private spying is a booming business. A rapidly growing sector of the surveillance economy involves the provision of spyware, a type of malware installed on someone's device without knowledge or consent. Spyware providers earn monthly fees for providing secret, real-time access to a networked device owner's communications and activities.¹

1. See Aarti Shahani, *Smartphones Are Used to Stalk, Control Domestic Violence Victims*, NPR (Sept. 15, 2014, 4:22 PM),

The “stalking app” is the private spy’s current tool of choice.² Search Google for “cell phone spy,” and an array of advertisements appear.³ “Worried about your spouse cheating? Track EVERY text, EVERY call and EVERY move they make using our EASY Cell Phone Spy Software,” explained one provider.⁴

The privacy invasions enabled by such surveillance software are breathtaking.

Some stalking apps are devoted to tracking a phone owner’s geolocation data—the street and city where a phone is present.⁵ Geolocation data tells us far more than points on a map. In her concurrence in *United States v. Jones*,⁶ Justice Sonia Sotomayor warned that monitoring a person’s public movements “reflects a wealth of detail about her familial, political, professional, religious, and sexual associations.”⁷

Other stalking apps offer an even more revealing picture of someone’s daily activities. With these apps, subscribers can monitor everything phone owners do with their devices. In real time, subscribers can listen to a phone owner’s calls and video chats; they can view their texts, photos, calendars, contacts, and

<http://www.npr.org/sections/alttechconsidered/2014/09/15/346149979/smartphones-are-used-to-stalk-domestic-abuse-victims> (last visited Sept. 20, 2015) (providing an overview of how smartphones are utilized to spy on domestic abuse victims) (on file with the Washington and Lee Law Review).

2. See Cahal Milmo, *Exclusive: Abusers Using Spyware Apps to Monitor Partners Reaches ‘Epidemic Proportions,’* THE INDEP. (Dec. 26, 2014), <http://www.independent.co.uk/news/uk/home-news/exclusive-abusers-using-spyware-apps-to-monitor-partners-reaches-epidemic-proportions-9945881.html> (last visited Sept. 20, 2015) (detailing the increasing popularity of spyware applications) (on file with the Washington and Lee Law Review).

3. See Appendix, Exhibit A (showing the results for such an internet search).

4. See *Location Privacy Protection Act of 2014: Hearing Before the Subcomm. on Privacy, Tech. and the Law of the S. Comm. on the Judiciary*, 113th Cong. (2014) (statement of Cindy Southworth, Vice President of the National Network to End Domestic Violence on behalf of the Minnesota Coalition for Battered Women) [hereinafter *Southworth Testimony*] (describing how spyware apps target domestic violence victims).

5. See *id.* (explaining how certain apps function).

6. 132 S. Ct. 945 (2012).

7. See *id.* at 955 (Sotomayor, J., concurring) (warning of the hazards of location monitoring).

browsing habits.⁸ Targeted phones can be turned into bugging devices; conversations within a fifteen-foot radius of a phone are recorded and uploaded to the provider's portal. As FlexiSpy tells subscribers, "[b]ug their room: listen in on their phone's surroundings and listen in on what is really going on behind closed doors."⁹

A key selling point of stalking apps is their hidden nature.¹⁰ Subscribers are assured that, once they download the spyware app to someone's phone, the phone owner will be unable to detect the spyware.¹¹ Stalking apps are advertised as "100% undetectable."¹² FlexiSPY promises "total control of your partner's phone without them knowing it. . . . See exactly where they are, or were, at any given date or time."¹³ Cellphone Spying stresses:

[w]hat this app . . . can do is capture that information for retrieval at a later date—without the target phone user ever knowing anything about it! As with all its functionality, the user of the targeted phone will have no clue that their phone has been compromised or that their data is getting leaked to somebody else.¹⁴

8. Saiyai Sakawee, *This App Lets Men with "Several Girlfriends" Spy on Their Significant Others' Every Move*, TECH IN ASIA (Dec. 11, 2013, 7:00 PM), <https://www.techinasia.com/app-lets-men-several-girlfriends-spy-significant-others-move/> (last visited Sept. 20, 2015) (listing the range of functions that applications offer) (on file with the Washington and Lee Law Review).

9. FLEXISPY, <http://www.flexispy.com> (last visited Sept. 20, 2015) (on file with the Washington and Lee Law Review).

10. See *id.* (marketing itself as a spy app).

11. mSpyVIP, *Cell Phone Spy – mSpy Review*, YOUTUBE (Dec. 15, 2012), <https://www.youtube.com/watch?v=YNbT0At4Tsg> (last visited Sept. 20, 2015) (detailing one such spyware app) (on file with the Washington and Lee Law Review).

12. See *Southworth Testimony*, *supra* note 4 (describing the advertising tactics of spyware apps).

13. See *Location Privacy Protection Act of 2014: Hearing Before the Subcomm. on Privacy, Tech. and the Law of the S. Comm. on the Judiciary*, 113th Cong. (2014) (statement of Chairman Franken) [hereinafter, *Franken Statement*] (discussing the tools that are advertised).

14. See *How Do Cell Spying Apps Work?*, CELLSPYINGHQ (Jan. 15, 2014), <http://cellspyinghq.com/how-do-cell-spying-programs-work/> (last visited Sept. 20, 2015) (detailing the apps' unique tools) (on file with the Washington and Lee Law Review).

HelloSpy claims that its app “silently monitor[s] text messages, GPS locations, call details, photos, and social media activity.”¹⁵ Users are assured that the app “does not display any icons and appears on the device application database under different names (system processes), which leaves virtually no chance for the user to identify this software.”¹⁶

Cyber stalking apps and their ilk thus enable continuous and secret tracking of a cell phone owner’s intimate conversations, medical appointments, online banking activity, intellectual musings, minute-to-minute movements, and far more. As the Court underscored in *Riley v. California*,¹⁷ with access to someone’s cell phone, a viewer can reconstruct the “sum of an individual’s private life.”¹⁸

Although providers often emphasize that parents and employers could use their apps to check on children and employees, stalkers and domestic abusers are often their targeted audience.¹⁹ National Network to End Domestic Violence’s (NNEDV) Vice President Cindy Southworth explains that “some developers try to mask their nefarious intentions by mentioning child safety or employee safety once or twice, but their true focus is obvious when they reiterate on every page how their products are completely hidden and work in stealth mode.”²⁰

If one digs at all, it becomes clear that stealth surveillance of ex-intimates is a key goal.²¹ Stalking apps are hailed as the “spy in

15. HELLOSPY, hellospy.com (last visited June 20, 2015) (on file with the Washington and Lee Law Review).

16. See *Southworth Testimony*, *supra* note 4 (explaining how the companies focus their advertising on the undiscoverability of the app).

17. 134 S. Ct. 2473 (2014).

18. See *id.* at 2489 (discussing the effects of long-term surveillance).

19. See Appendix, Exhibit B (showing an advertisement targeting individuals interested in spying on their spouses).

20. *Senate Bill Would Ban Stalking Apps and Save Women’s Lives*, NAT’L NETWORK TO END DOMESTIC VIOLENCE (June 4, 2014), <http://nnedv.org/news/4296-senate-bill-would-ban-stalking-apps-and-save-women-s-lives.html> (last visited Sept. 20, 2015) (on file with the Washington and Lee Law Review).

21. Cellphone Spying, a site about stealth spying on intimates, links to PhoneWatcher.net, which in turn links to the spyware provider mSpy. mSpy says that 40% of users are parents and 10 to 15% are small businesses monitoring employees but is silent about the remaining 45 to 50% of its customers. See Kate Knibbs, *Smartphone Spying Startup Will Keep an Eye on NYC*, DAILY DOT (Feb.

[a cheating spouse's] pocket.”²² FlexiSPY advertisements prominently feature a photo of a couple next to the message: “many spouses cheat. They all use cell phones. Their phones will tell you what they won’t.”²³ The advertisement continues, “Women who do cheat usually do so in a well-planned and discrete [sic] fashion, making it exceedingly difficult for their man to know they’re being cuckolded. . . . Women are much more capable of looking you straight in the eye and lying.”²⁴ A marketing video for a stalking app asked, “So you want to keep an eye on your loved one or your employees, because you suspect they’re hiding something and it might get too late?”²⁵ Another app provider’s advertisement includes “a photo of a woman whose face was marked with ugly abrasions and whose forearm was held in the grip of a man.”²⁶ Finally, mSpy emphasizes that its software app helps people catch cheating wives.²⁷

Much of this activity is illegal.²⁸ Intercepting electronic communications without at least one party’s consent violates

27, 2014), <http://www.dailydot.com/technology/mspy-goes-to-nyc/> (last visited Sept. 20, 2015) (discussing how various spy apps are intertwined) (on file with the Washington and Lee Law Review). In March 2014, mSpy’s website demonstrated the service with a man tracking the communications and whereabouts of his wife and son. See E.J. Dickson, *To Catch a Cheater: 6 Apps for Spying on Your Significant Other*, DAILY DOT (Mar. 5, 2014), <http://www.dailydot.com/technology/love-surveillance-spying-apps/> (last visited Sept. 20, 2015) (listing spy apps that are currently available and the services offered by each) (on file with the Washington and Lee Law Review).

22. See Dickson, *supra* note 21 (discussing the advertising techniques used by various apps).

23. FLEXISPY, *supra* note 9. Under the caption “Catch Cheaters,” Flexispy asks, “Is your wife or husband cheating on you? For the sake of your mental and sexual health, you have a right to know if your partner is being responsible. Spy on their cellphones to know.” *Id.*

24. Milmo, *supra* note 2.

25. STEALTH GENIE, *StealthGenie—World’s Most Powerful Cell Phone Spy Software*, YOUTUBE (2013), <http://www.youtube.com/watch?v=YycVKHOCp0M&list=UUi2qZEeLu4x7-eH70o52njQ> (last visited Sept. 20, 2015) (on file with the Washington and Lee Law Review).

26. Kim Zetter, *The Criminal Indictment That Could Finally Hit Spyware Makers Hard*, WIRED (Oct. 1, 2014), <http://www.wired.com/2014/10/stealthgenie-indictment/> (last visited Sept. 20, 2015) (on file with the Washington and Lee Law Review).

27. See mSpyVIP, *supra* note 11 (advertising the benefits of its application).

28. See *infra* note 132 (listing various state statutes regulating cyber

federal and state wiretap laws.²⁹ At the federal level, and in most states, cyber stalking is a crime.³⁰ But, bringing criminal law to bear against individual perpetrators is challenging. Spyware apps are hard to detect; so then is the criminal surveillance.

Even when stalking victims suspect that their phones are being monitored, their complaints to law enforcement are seldom pursued. Police departments often lack the forensic equipment necessary to examine mobile devices for stalking apps.³¹ Reports often go nowhere because domestic violence and stalking are low priorities for law enforcement. Police officers receive little training on the relevant laws and the technology necessary to investigate such crimes.³² Because both the law and the technology are not well understood, law enforcement does little beyond advising victims to get rid of their phones.³³ Resources to fund digital forensic investigations are especially scarce at the state and local level.³⁴ Then too, the lack of cooperation between jurisdictions may prevent the apprehension of stalkers.³⁵

What about the parties responsible for providing spyware and other covert surveillance tools? Under federal law, it is a crime to manufacture, sell, or advertise a device knowing or having reason

surveillance).

29. See *infra* note 132 (listing the ways in which states have attempted to regulate the monitoring of cyber communications).

30. DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE 123–25 (2014).

31. *Location Privacy Protection Act of 2014: Hearing Before the Subcomm. on Privacy, Technology and the Law of the S. Comm. on the Judiciary*, 113th Cong. (2014) (statement of Detective Brian Hill, Criminal Investigations Division, Anoka County Sheriff's Office) [hereinafter *Hill Testimony*].

32. See CITRON, *supra* note 30, at 83–87 (exploring the ways in which law enforcement officials handle cyber stalking). The Attorney General of California Kamala Harris has been working hard to address this problem in her state. I am working with her Task Force on Cyber Exploitation on efforts to educate law enforcement about cyber stalking. Funds are being diverted to enhance law enforcement's digital forensic expertise in California. Telephone Interview with then Special Attorney General Jeffrey Rabkin (notes on file with author).

33. See *id.* at 83–85 (discussing the issues that law enforcement officials face when dealing with cyber stalking).

34. See *id.* at 88–89 (explaining the various challenges that plague law enforcement).

35. See *id.* (noting the coordination required between agencies for successful enforcement of cyber-related laws).

to know that the design of the device renders it “primarily useful” for the covert interception of electronic, wire, or oral communications.³⁶ Twenty-five states and the District of Columbia have similar criminal statutes.³⁷ At least in theory then, the providers of stalking apps could face federal and state criminal charges if it can be proved beyond a reasonable doubt that they knew or had reason to know the apps were designed to be “primarily useful” for secret surveillance.

The prosecution of businesses involved in the manufacture and sale of stalking apps could be a crucial deterrent, but that possibility has not yet been realized. There have been few, if any, state prosecutions against the entities providing covert surveillance tools and a modest number at the federal level. If law enforcement initiated more investigations, the law might only cover a narrow set of devices or tools: those whose design renders them “primarily useful” for the interception of electronic, wire, or oral communications. Existing law does not ban the interception of location data.

Although the Federal Trade Commission has brought a handful of enforcement actions against spyware providers for engaging in unfair and deceptive trade practices, and a few state Attorneys General have done the same, stalking app providers have paid little attention.³⁸ Such services continue to proliferate; their ads brazenly appear online.³⁹

Something more must be done. Software secretly tracking a phone’s activities exacts profound costs to privacy while serving no legitimate purpose. Aided by spyware, abusers can find victims who are desperately trying to escape them. Victims of domestic abuse have been beaten and killed. When victims learn that their phones are the source of their vulnerability, the emotional fallout is profound. Stalking victims lose their sense of personal safety. They experience anxiety at the thought of being under surveillance

36. 18 U.S.C. § 2512 (2012).

37. See *infra* note 132 (listing the various state codes).

38. See *infra* Part III.B. (discussing various law enforcement efforts including those by the Federal Trade Commission).

39. See Exhibits A, B (displaying two stereotypical online advertisements for stalking apps).

by their stalkers. New phones must be purchased, and time must be spent devising new passwords and accounts.⁴⁰ Many victims lack the resources to purchase new phones. If an abuser tracks a domestic violence victim to a shelter, other victims staying at the shelter are at risk.⁴¹

Domestic abusers and stalkers are increasingly turning to surveillance software to terrorize victims. A Bureau of Justice Statistics study conducted in 2006 estimated that 25,000 people are stalked via GPS annually.⁴² That number surely understates the problem given the increasing adoption of cell phones and availability of stalking apps.⁴³ Consider these studies. The National Network to End Domestic Violence found that 71% of domestic abusers monitor survivors' computer activities, and 54% of abusers tracked survivors' cell phones with stalking apps.⁴⁴ According to a 2012 survey of 750 victim services agencies, 75% of domestic violence survivors experience tracking of their location through their cell phones or a GPS device.⁴⁵ A 2014 study sponsored by Digital Trust found that more than 50% of abusive partners used spyware or some other form of electronic surveillance to stalk victims.⁴⁶ The overall number of stalking victims is significant and growing; in 2009, the Bureau of Justice Statistics estimated that over 3.4 million individuals are stalked annually;⁴⁷ in 2014, the Department of Justice's Bea Hanson testified that 6.6 million people are stalked annually.⁴⁸

40. See *Hill Testimony*, *supra* note 31 (discussing how individuals handle being targets of surveillance).

41. Much thanks to Rachel Levinson-Waldman for her expertise and insights on these matters.

42. KATRINA BAUM, SHANNA CATALANO, MICHAEL RAND & KRISTINA ROSE, *STALKING VICTIMIZATION IN THE UNITED STATES* 8 (2009).

43. The Department of Justice may no longer be a resource for data about GPS stalking. Unfortunately, the Bureau of Justice Statistics survey has eliminated inquiry into the prevalence of GPS stalking.

44. SAFETY NET TECHNOLOGY SAFETY SURVEY, A GLIMPSE FROM THE FIELD: HOW ABUSERS ARE MISUSING TECHNOLOGY, NATIONAL NETWORK TO END DOMESTIC VIOLENCE (2014).

45. *Southworth Testimony*, *supra* note 4.

46. Milmo, *supra* note 2.

47. BAUM, *supra* note 42, at 8.

48. *Location Privacy Protection Act of 2014: Hearing Before the Subcomm. on*

Despite the dangers, surveillance software remains widely available for purchase by domestic abusers and stalkers.⁴⁹ The risks of stalking apps will only escalate over time as our smart phones are connected to even more revealing information, such as biometric measuring devices and home appliances.

This Essay proposes a legal agenda aimed to curtail the enablers of private spies—the businesses manufacturing, selling, or advertising spyware and other stealth surveillance equipment. Given the difficulty of finding stalkers due to the surreptitious nature of surveillance tools, the producers of such software are a crucial source of punishment and deterrence. The question is how might we improve the law, its enforcement, and other non-legal efforts.

Legal reforms are needed to combat the production of cyber stalking apps. Current criminal law may be too narrow and overly restrictive to combat the stalking app industry. The provision of devices secretly collecting location data should be banned. Also, criminal law should extend to the purveyors of devices whose design renders them “useful” for secret surveillance. Another potential reform is to require app providers to collect records on subscribers so that private spies can be found and caught. On the civil side, individuals should be given a private right of action against the purveyors of cyber stalking software.

Legal reform should be paired with efforts to enhance law enforcement. More resources should be dedicated to training law enforcement and to digital forensic expertise. Criminal law has no chance of serving as a deterrent if it is never pursued. State Attorneys General should prioritize enforcement actions against spyware providers under their unfair and deceptive practice laws.

To be clear about this paper’s scope, this Essay does not address government surveillance. In a series of articles, David Gray and I have explored government’s mass data collection, analysis, and sharing.⁵⁰ We have proposed a right to quantitative

Privacy, Tech. and the Law of the S. Comm. on the Judiciary, 113th Cong. (2014) (statement of Bea Hanson, Principal Deputy Dir., Dep’t of Justice Office of Violence Against Women).

49. BAUM, *supra* note 42, at 8.

50. See generally David Gray & Danielle Keats Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62 (2013); David Gray & Danielle Keats

privacy to strike a better balance between individual and collective expectations of privacy and law enforcement's interest in preventing, detecting, and prosecuting terrorism and crimes. This Essay leaves aside the collection, use, and sharing of personal data for legitimate commercial ends, which I have explored in other work.

Part II sets the stage with a brief history of the industry involved in the secret surveillance of individuals' confidential communications. It discusses the development of tools facilitating the continuous, indiscriminate, and secret surveillance of individuals for private, criminal ends. Part III asks what current law does about the production of surveillance tools. It explores the gaps in legal protections and the under-enforcement of existing law. Part IV offers a legal agenda to combat the problem of private spying. It calls for an expansion of criminal and civil law and for more training and resources to ensure the enforcement of existing laws. Part IV concludes by addressing potential non-legal strategies.

II. The Private Surveillance Business

A. Evolution of the Spying Trade

Human beings are inherently curious. Gossip has long been a common pastime.⁵¹ Predictably then, as soon as telegraphs and telephones became available for purchase, so did devices designed to intercept confidential telephone and telegraph communications.⁵² In the early 1900s, telephone wiretap devices

Citron, *A Shattered Looking Glass: The Pitfalls and Potential of the Mosaic Theory of Fourth Amendment Privacy*, 14 N.C. J. L. & TECH. 381 (2013); David Gray, Danielle Keats Citron & Liz Clark Rinehart, *Fighting Cybercrime After United States v. Jones*, 103 J. CRIM. L. & CRIMINOLOGY 745 (2013); Danielle Keats Citron & David Gray, *Addressing the Harm of Total Surveillance: A Reply to Professor Neil Richards*, 126 HARV. L. REV. FORUM 262 (2013); Danielle Keats Citron & Frank Pasquale, 62 *Network Accountability for the Domestic Surveillance State*, 62 HASTINGS L.J. 1441 (2011).

51. See generally DANIEL J. SOLOVE, *THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET* (2007) (exploring the history of gossip).

52. See SAMUEL DASH, *THE INTRUDERS: UNREASONABLE SEARCHES AND SEIZURES FROM KING JOHN TO JOHN ASHCROFT* 79 (2004) (providing a history of

were widely advertised and sold.⁵³ Businesses and individuals bought them to spy on competitors, employees, and spouses.⁵⁴

Over time, spying tools grew in variety and sophistication.⁵⁵ In the 1940s and 1950s, mail order catalogs sold location trackers, spy cameras, bugging devices, radio pills, and tiny tape recorders.⁵⁶ Available for purchase were bugging devices hidden in martini olives, suitcase handles, earrings, and tie clasps.⁵⁷ Miniature bugging devices could broadcast conversations to a receiver a block away.⁵⁸ Parabolic microphones could pick up voices without being placed on the premises.⁵⁹ Catalogs sought to avoid entanglement with the law by warning buyers to use bugging tools “according to the laws of your community.”⁶⁰

The low cost of spying devices fueled their widespread adoption.⁶¹ Businesses installed microphones in the walls of employee restrooms and desks.⁶² Model homes and car salesrooms were equipped with hidden bugs to allow salespeople to overhear the musings of prospective buyers.⁶³ Husbands bugged their wives’

surveillance devices throughout history). During the Civil War, military telegraph messages were routinely intercepted. *Id.* After the war’s end, telegraph operators got into the private wiretapping business. *Id.*

53. Alan F. Westin, *The Wire-Tapping Problem: An Analysis and a Legislative Solution*, 52 COLUM. L. REV. 165, 168 (1957).

54. *Id.*

55. See DASH, *supra* note 52, at 85 (providing a history of surveillance techniques); see also *Berger v. New York*, 388 U.S. 41, 47 (1967) (discussing the expansion of “detection techniques”).

56. See ALAN WESTIN, *PRIVACY AND FREEDOM* 90, 98 (1967) (discussing surveillance tools available over the decades).

57. See *id.* (listing the various products available to consumers).

58. See MYRON BRENTON, *THE PRIVACY INVADERS* 152 (1964) (discussing the efficacy of certain surveillance devices).

59. See *Berger*, 388 U.S. at 47 (explaining how the technology used functions in practice).

60. See BRENTON, *supra* note 58, at 155 (discussing how surveillance technology was advertised in the past).

61. To the tune of \$250. *Id.* at 153.

62. See DASH, *supra* note 52, at 84 (discussing how businesses took advantage of new surveillance technology).

63. See *id.* at 85 (explaining how businesses could use surveillance devices for their own commercial advantage).

bedrooms and wiretapped their home phones; wives wiretapped and bugged their husbands' offices.⁶⁴

Early bugging devices faced objections and legal restrictions. As Part II explores, states and Congress barred nonconsensual wiretapping, but the laws were limited in their reach and hardly ever enforced.

B. Private Spying 2.0

The martini listening device, telephone bug, and parabolic microphone are quaint by modern standards. Today's spying tools can provide a comprehensive picture of someone's minute-to-minute activities, from the sacred to the quotidian. In a dragnet style, they produce a continuous record of a person's movements, communications, online browsing, reading habits, searches, snapchats, videos, and more in real time.⁶⁵ Thanks to falling storage costs, it is cheap to preserve a continuous record of our intellectual, economic, political, social, and physical pursuits.

Cell phones are gold mines for the spying business. Every time a person's phone generates media content, the content is uploaded to the spyware subscriber's account for remote viewing. Through a web portal, users can view the person's calendar entries, Facebook posts, address book, photos, videos, online activities, text messages, call logs, emails, snapchats, and location. The watcher can turn the person's phone into a bugging device and pick up his or her conversations.⁶⁶ Cell phone owners will have no reason to suspect the surveillance because spyware is designed to be undetectable.⁶⁷

In the near future, far more information will be linked to mobile personal devices. Already on the market are fitness exercise

64. See *id.* (noting that surveillance devices also had an impact domestically).

65. See Part II (introducing various cyber surveillance applications and how they operate).

66. See Knibbs, *supra* note 21 (discussing the powers given to an individual using spyware).

67. United States' Memorandum of Law in Support of Motion for Preliminary Injunction at 4, *United States v. Akbar*, 2014 WL 7692300 (No. 1:14-CV-1273), (E.D. Va. Oct. 2, 2014).

bands that link to our phones, tracking our heart rate and exercise. Soon, cell phones will be connected to our home appliances, alarms, and more.

We have some sense of the businesses involved in spyware.⁶⁸ Let's consider a few examples. mSpy, a U.K. company with a New York office, sells a mobile app that facilitates the stealth monitoring of a person's phone activity. According to mSpy, 74% of its users are male. The most active users are between thirty-five to forty-four years old, and 53% live in the United States. Texans and Californians drive the most traffic to mSpy's website.⁶⁹ mSpy says that parents make up 40% of its users and that employers constitute 10 to 15% of its user base. mSpy has said nothing about the remaining 45 or 50% of its customers. In March 2014, mSpy's website demonstrated the service with a man tracking the communications and whereabouts of his wife and son.⁷⁰

Highster Mobile allows users to "secretly track and spy on virtually any cell phone quickly and easily completely undetected."⁷¹ On YouTube, a Highster Mobile subscriber hailed the spyware for helping him catch his wife cheating: "Without this software, I would not have been able to know that my suspicions about her cheating was [sic] correct."⁷² A Highster Mobile-sponsored user review page included several reviews applauding the app's utility in stalking intimates. One person wrote, "It doesn't work very well, but [I] did receive enough text messages to know she is cheating on me, not with 1 guy but 3, what a

68. Just to name a few: iSpyoo, SpyBubble, Highster, mSpy, Cell Phone Spy, and Spy to Mobile. Leah Wightley, *Highster Mobile Review*, YOUTUBE (Aug. 19, 2014), <https://www.youtube.com/watch?v=O2Bs5ABMRoA> (last visited Sept. 20, 2015) (on file with the Washington and Lee Law Review).

69. Molly Mulshine, *Watch What You Text: iPhone Surveillance Startup Moves to NYC*, BETABEAT (Feb. 26, 2014), news.yahoo.com/watch-text-iphone-surveillance-startup-moves-nyc-220815427.html (last visited Sept. 20, 2015) (on file with the Washington and Lee Law Review).

70. Dickson, *supra* note 21.

71. *Remote Cell Phone Tracker and Spy*, HIGHSTER MOBILE, <http://www.highstermobi.com> (last visited Sept. 20, 2015) (on file with the Washington and Lee Law Review).

72. lousieramirez88, *Best Cell Phone Spying Tool, How I Find Out that My Wife Was CHEATING!!*, YOUTUBE (Feb. 9, 2013), <https://www.youtube.com/watch?v=X0CIhdDbChY> (last visited Sept. 10, 2015) (on file with the Washington and Lee Law Review).

woman!!”⁷³ Still another said, “Highster Mobile literally changed my life after I found my suspicions were correct. I’m now living in a different country and having the time of my life. I am free!!!”⁷⁴ YouTube users reviewing the app said it is great to use to watch your “cheating spouse” or your kids.⁷⁵

C. Perils of Spyware

Spyware apps allow stalkers and domestic abusers to terrorize victims. Physical harm is a serious peril when abusers have access to victims’ activities and whereabouts. A woman fled her abuser with whom she was living in Kansas.⁷⁶ Because the woman’s abuser had installed a cyber-stalking app on her phone, he knew that she had moved to Elgin, Illinois.⁷⁷ The man tracked the woman to a shelter and then a friend’s home where he assaulted her.⁷⁸ In another case, a woman tried to escape her abusive husband, but because he had installed a stalking app on her phone, he was able to find her and her children. After tracking them down, the man murdered his two children.⁷⁹ In 2013, a California man, using a spyware app, tracked a woman to her friend’s house and attacked her.⁸⁰

In addition to the serious physical risks posed by abusers’ access to spyware, imagine the chilling of expression and anxiety that ensues when stalking victims discover that their abusers have real-time access to their communications, searches, photos, books on reading apps, snapchats, social network messages, activity on

73. *Highster Mobile Reviews*, TOP 10 SPY SOFTWARE REV., <http://www.top10spysoftware.com/review/highstermobile> (last visited June 20, 2015) (on file with the Washington and Lee Law Review).

74. *Id.*

75. Highster Mobile Review, *Highster Mobile 3: What You Need to Know Before You Buy Highster Mobile*, YOUTUBE (Jan. 29, 2014), <https://www.youtube.com/watch?v=aUvvVx06iLw> (last visited Sept. 20, 2015) (on file with the Washington and Lee Law Review).

76. *Franken Statement*, *supra* note 13.

77. *Id.*

78. *Id.*

79. *Id.*

80. *Southworth Testimony*, *supra* note 4.

dating apps, and steps taken—for days, weeks, and months. According to NNEDV's Cindy Southworth, abusers' goal is to assert control over victims, and it works.⁸¹ As victims have told law enforcement, even if they obtain new phones, they no longer feel safe using them. What is to stop their abusers from reinstalling spyware on their phones? Victims become paranoid about using networked technologies for work, socializing, and public conversations, lest their abusers track them down. They experience distress about being watched.⁸²

That sort of chilling implicates our intellectual privacy.⁸³ Once individuals become aware that their communications have been under surveillance, they may internalize the notion of being listened to and watched. Individual development is inevitably stunted in the face of unwanted monitoring.

Finally, stalking apps can be used to facilitate financial crimes. For instance, they can be used to steal sensitive personal information like social security numbers and passwords to assist in identity theft. Secretly installed spyware provides users access to a victim's bank passwords that can be used to empty accounts.⁸⁴ If victims lose their financial cushion, the harm that they experience will be far worse and their options more limited.⁸⁵

81. Aarti Sahani, *Domestic Abusers Use Cellphones to Stalk, Abuse, and Control*, NAT'L PUB. RADIO (Sept. 15, 2014), <http://www.npr.org/sections/alltechconsidered/2014/09/15/346149979/smartphones-are-used-to-stalk-control-domestic-abuse-victims> (last visited Sept. 20, 2015) (on file with the Washington and Lee Law Review).

82. Studies have shown that people experience anxiety about being watched and misunderstood. See generally Stuart A. Karabenick & John R. Knapp, *Effects of Computer Privacy on Help-Seeking*, 18 J. APPLIED SOC. PSYCHOL. 461 (1988) (analyzing the effects of cyber surveillance).

83. See generally NEIL M. RICHARDS, *INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE* (2015); JULIE E. COHEN, *CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY LIFE* 141 (2012); Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934 (2013); Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387 (2008); Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1425–26 (2000).

84. Preliminary Injunctive Order, *F.T.C. v. CyberSpy Software LLC*, No. 08-CV-01872 (M.D. Fla. Nov. 25, 2008), available at <http://www.ftc.gov/sites/default/files/documents/cases/2008/11/081128cyberspyi.pdf>.

85. *Southworth Testimony*, *supra* note 4, at 15.

III. Law's Role Combating Spying Inc.

"Few threats to liberty exist . . . greater than that posed by . . . eavesdropping devices."⁸⁶

Congress and half of the states have adopted bans on the business side of illegal eavesdropping, but the enforcement of those laws has been lackluster. This Part begins by laying out some key developments in wiretapping law. Then, it highlights federal and state prohibitions on the manufacture, sale, and advertisement of certain surveillance devices. The enforcement of those laws and their limits are explored. This Part ends by discussing the role that federal and state consumer protection agencies have begun to play in curtailing the production of spyware.

A. Historical Development of Wiretapping Laws

In the mid-nineteenth century, a handful of states banned surreptitious wiretapping of telegraph communications. California passed the first criminal prohibition in 1862.⁸⁷ Telegraph wiretapping bans were soon extended to include wiretaps on telephones.⁸⁸

The Supreme Court heard its first wiretapping case in 1928. In *Olmstead v. United States*,⁸⁹ Chief Justice Taft, writing for the majority, ruled that government interception of private telephone communications did not implicate the Fourth Amendment's prohibition of unreasonable searches and seizures.⁹⁰ The Court reasoned that "projected voices" did not constitute "actual physical invasions" of the home warranting Fourth Amendment protection.⁹¹ Because government agents cut into defendant's telephone wires outside his home and had not trespassed inside it,

86. *Berger v. New York*, 388 U.S. 41, 63 (1967).

87. *Id.* at 45–46.

88. *Id.* California extended its prohibition of telegraph wiretapping to telephone wiretapping in 1905. DASH, *supra* note 52, at 81.

89. 277 U.S. 438 (1928).

90. *See id.* at 466 ("[T]he wiretapping here disclosed did not amount to a search or seizure within the meaning of the Fourth Amendment.").

91. *Id.*

no Fourth Amendment violation had occurred, the Court held.⁹² The fact that federal law enforcement had violated state wiretapping law was irrelevant.⁹³

As the Court noted in *Olmstead*, Congress could ban warrantless wiretaps to fill in the gaps left by the Constitution.⁹⁴ Federal lawmakers did just that in the Federal Communications Act of 1934.⁹⁵ Section 605 of the Communications Act banned the interception of radio or wire communications and the disclosure of the content of such communications absent the consent of one of the parties.⁹⁶ The use of devices to secretly record face-to-face communications in private places was not banned.⁹⁷

As a practical matter, the Communications Act offered scant protection against wiretapping. The Department of Justice interpreted § 605 to mean that law enforcement could engage in wiretapping if it did not divulge material obtained via wiretaps to others.⁹⁸ Because that interpretation was backed by judicial decisions, law enforcement regularly used wiretapping equipment in investigations. Private parties rarely faced prosecution under either federal or state law because it seemed difficult to justify

92. *Id.*

93. *See id.* at 468–69 (“Whether the state of Washington may prosecute and punish federal officers violating this law . . . is not before us.”).

94. *Id.* at 465. Justice Brandeis wrote a powerful dissent that took the majority to task for linking Fourth Amendment protection to outmoded property rights. *Id.* at 473–74 (Brandeis, J., dissenting). A property-based approach failed to protect citizens from procedures that might not require the “force and violence” necessary to invade property, but nonetheless compromised the sanctity of citizens’ thoughts, beliefs, emotions as well as the “individual security” they invested in activities like telephone conversations. *Id.* at 473–74, 478–79 (Brandeis, J., dissenting). As Justice Brandeis underscored, telephone communications are more private and confidential than tangible objects in the home. Compared to telephone wiretaps, general warrants and writs of assistance were “but puny instruments of tyranny and oppression.” *Id.* at 476. Fourth Amendment understandings needed to evolve to address scientific advances that permitted government agents to invade our most private and intimate information without physically intruding on the home.

95. 47 U.S.C. §§ 151–615(b) (2012).

96. *Id.* § 605.

97. DASH, *supra* note 52, at 83.

98. WESTIN, *supra* note 56, at 177.

criminal charges against individuals when law enforcement engaged in the same activity.⁹⁹

In 1967, two Supreme Court decisions—*Katz v. United States*¹⁰⁰ and *Berger v. New York*¹⁰¹—changed the trajectory of electronic surveillance law. In those cases, the Supreme Court overturned *Olmstead*, ruling that electronic surveillance constituted a search and seizure governed by the Fourth Amendment.¹⁰² Under *Katz*, surveillance focused on the interception of a few conversations was constitutionally acceptable if the interception was approved by a judge and based on a special showing of need.¹⁰³ By contrast, lengthy, continuous, and indiscriminate electronic surveillance violated the Fourth Amendment.¹⁰⁴

Katz involved an investigation of a man allegedly running an illegal betting operation.¹⁰⁵ Agents listened to the man's calls by attaching a suction microphone to a telephone booth's roof.¹⁰⁶ *Katz* was convicted based on evidence gathered by the microphone.¹⁰⁷ The Court held that using a listening device to monitor telephone conversations in a public phone booth constituted a Fourth Amendment "search."¹⁰⁸ In rejecting the trespass requirement, the Court declared that "the Fourth Amendment protects people, not places."¹⁰⁹ The Court found that conversations in telephone booths

99. *Id.* at 179, 186.

100. 389 U.S. 347 (1967).

101. 388 U.S. 41 (1967).

102. *Id.* at 50–82.

103. See generally James X. Dempsey, *Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy*, 8 ALB. L.J. SCI. & TECH. 65 (1997).

104. *Berger v. New York*, 388 U.S. 41 (1967).

105. See *Katz v. United States*, 389 U.S. 347, 348–49 (1967) (providing the facts of the case).

106. See *id.* (describing how the FBI had obtained evidence in the case).

107. See *id.* at 353 ("The Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment.").

108. See *id.* (finding that the government had violated *Katz*'s reasonable expectation of privacy).

109. *Id.* at 351.

deserve Fourth Amendment protection because citizens expect that their telephone conversations are just as secure from public review as their daily routines in the home.¹¹⁰ The Court noted that phone booths function as spaces of aural repose.¹¹¹ Citizens could reasonably expect that their conversations in telephone booths would not be monitored by “uninvited ear[s],” even if they can be seen by “intruding eye[s].”¹¹² Declining to extend Fourth Amendment protection would unsettle these broadly held expectations and raise the specter of a surveillance state.¹¹³ In *Berger*, the Court made clear that “the fantastic advances in the field of electronic communication constitute a great danger to the privacy of the individual.”¹¹⁴ The Court held that wiretapping statutes needed to include special privacy protections for governmental monitoring to pass constitutional muster because the indiscriminate nature of electronic surveillance devices was reminiscent of the reviled general warrant.¹¹⁵

In the shadow of *Berger* and *Katz*, Congress passed the Title III Wiretap Act of 1968 and the Electronic Communications Privacy Act (ECPA) of 1986.¹¹⁶ Title III laid out a regime of protections “to compensate for the uniquely intrusive aspects of electronic surveillance.”¹¹⁷ Law enforcement had to meet stringent warrant requirements to intercept telephone calls over the wires.

110. *See id.* at 351–52 (emphasizing the expectation of privacy).

111. *Id.*

112. *Id.* at 352.

113. *Id.* at 354–59.

114. *Berger v. New York*, 388 U.S. 41, 41–62 (1967).

115. *See id.* at 47 (ruling that wiretapping raised special Fourth Amendment concerns because it involved continuous intrusions, searches, seizures, and the indiscriminate monitoring of communications over a period of time without connection to the crime under investigation, unlike the limited intrusion of a traditional search).

116. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197. The Electronic Communications Privacy Act extended the Title III’s protections to wireless voice communications and voice communications of a non-voice nature, such as e-mail or other computer-to-computer transmissions.

117. Dempsey, *supra* note 103, at 71. *See* Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. PA. L. REV. 373, 379 (2014) (discussing provisions of Title III that provide exceptions when wiretapping is legal without a court order and set forth procedures for lawful interception pursuant to a court order).

Law enforcement could obtain wiretap orders only on a showing of special need, a predicate felony offense, and high-level Justice Department or state approval.¹¹⁸ Wiretap orders had to be narrowly tailored and time limited.¹¹⁹ Officers had to “minimize” the interception of innocent conversations.¹²⁰ Such minimization was deemed essential to satisfy the Fourth Amendment’s particularity requirement, making up for the fact that law enforcement was getting access to all of the target’s communications, including those unconnected to the crime under investigation.¹²¹ Wiretaps falling short of these requirements were banned.¹²²

B. Cutting Off the Source: Section 2512 and Analogous State Statutes

Congress did not focus solely on government surveillance. Federal lawmakers made it a crime for private individuals to engage in secret wiretapping. Under Title III, it is a felony to intercept electronic communications unless one of the parties to a communication consented to the interception.¹²³ In passing Title III, legislators recognized that private spies would be difficult to identify. After all, eavesdropping equipment is designed to ensure that those under surveillance do not know about it.

To enhance Title III’s deterrent effect, Congress included a provision covering those involved in the manufacture, sale, and advertisement of covert surveillance devices. The idea was to “dry

118. See Kerr, *supra* note 117, at 380.

119. See 18 U.S.C. § 2518(3), (5) (2012) (requiring that orders authorizing wiretaps be for the shortest duration necessary).

120. *Id.* § 2518(5).

121. Dempsey, *supra* note 103, at 70.

122. For a thoughtful exploration of the significance of Title III and *Katz*, see generally Susan Freiwald, *A First Principles Approach of Communications’ Privacy*, 2007 STAN. TECH. L. REV. 3 (2007).

123. 18 U.S.C. § 2511 (2012). Most states follow this approach, though twelve states criminalize the interception of electronic communications unless both parties to the communication consent to the interception. Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 U. ILL. L. REV. 1417, 1485 (2009).

up the source of equipment highly useful for surveillance.”¹²⁴ Section 2512 made it a crime to intentionally manufacture, sell, or advertise a device knowing or having reason to know that its design renders it “primarily useful” for the surreptitious interception of wire, oral, or electronic communications.¹²⁵ Defendants face fines of not more than \$10,000 or imprisonment of not more than five years or both.

Section 2512 covers a “narrow category of devices whose *principal use* is likely to be for wiretapping or eavesdropping.”¹²⁶ A surveillance device must be “sufficiently invasive or devious in purpose to warrant criminal prosecution.”¹²⁷ The inquiry focuses on the degree to which a device’s components render it useful for the secret interception of communications.¹²⁸ Disclaimers that customers should be advised of the law do not immunize defendants from conviction.¹²⁹ A defendant cannot avoid penalties under § 2512 “by surrounding himself with disclaimers and closing his eyes to the [surreptitious] nature and use of the devices.”¹³⁰

Section 2512’s safe harbor exempts entities that supply surveillance equipment to government agencies or communication providers.¹³¹ For instance, the manufacture of network packet sniffers seemingly falls outside of § 2512 because the device helps broadband providers detect network intrusion attempts, identify misuse by internal and external users, monitor network usage, and filter suspect content from network traffic. The provision of packet

124. S. REP. NO. 90-1097, at 2183 (1968).

125. 18 U.S.C. § 2512(1)(b) (2012).

126. *United States v. Shriver*, 989 F.2d 898, 906 (7th Cir. 1992) (quoting 1968 U.S. Code Cong. & Admin. News at 2112, 2183–84). Although Title III did not provide examples of devices on lawmakers’ minds, the Senate Report accompanying the statute included a non-exhaustive list of banned devices like the martini olive transmitter, spike mike, and microphones hidden in pens and calculators. *Id.* at 2112, 2184.

127. *Id.*

128. *Id.* That inquiry focuses on the “particular characteristics of the device at issue.” *Id.* Expert testimony may be useful to prove that a device is primarily designed for stealth use. *United States v. Wynn*, 633 F. Supp. 595, 602 (C.D. Ill. 1986).

129. *United States v. Brio*, 143 F.3d 1421, 1429 (11th Cir. 1998).

130. *Wynn*, 633 F. Supp. at 606.

131. 18 U.S.C. § 2512(2)(a), (b) (2012).

sniffers does not run afoul of the law because it is used in the normal course of a communication provider's business.

Twenty-five states and the District of Columbia have adopted similar statutes.¹³² Most state laws track the exact language of § 2512, including its safe harbor provisions. Pennsylvania makes it a felony to intentionally manufacture, sell, distribute, or advertise an “electronic, mechanical or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of a wire, electronic or oral communication.”¹³³ Maine's statute is broader; it proscribes the sale of “any device, contrivance, machine or apparatus designed or commonly used for the interception of wire or oral communications.”¹³⁴

As technology has evolved, gaps in the law have become apparent. Federal and state laws do not cover surveillance tools devoted to the secret collection of location data. As U.S. Senator Al Franken has admonished and worked to change, “there is no federal law banning the secret collection of location data.”¹³⁵ At the state level, the rare exception is Section 637.7 of the California Penal Code, which states that “[n]o person or *entity* in this state shall use an electronic tracking device to determine the location or movement of a person.”¹³⁶ This provision (and the few others like

132. ALA. CODE § 13A-11-34 (2015); CAL. PENAL CODE § 635 (West 2015); COLO. REV. STAT. § 18-9-302 (2015); CONN. GEN. STAT. § 54-41s (2015); DEL. CODE tit. 11, § 2403 (2015); D.C. CODE § 23-543 (2015); FLA. STAT. § 934.04 (2015); GA. CODE ANN. § 16-11-63 (West 2015); HAW. REV. STAT. § 803-43 (2015); IDAHO CODE ANN. § 18-6703 (West 2015); LA. REV. STAT. ANN. § 15:1304 (2015); ME. STAT. tit. 15, § 710 (2015); MD. CODE ANN., CTS. & JUD. PROC. § 10-403 (2015); MICH. COMP. LAWS § 750.539f (2015); MINN. STAT. § 626A.03 (2015); N.H. REV. STAT. ANN. § 570-A:3 (2015); N.J. STAT. § 2A:156A-5 (West 2015); N.C. GEN. STAT. § 15A-288 (2015); N.D. CENT. CODE § 12.1-15-03 (2015); OKLA. STAT. tit. 13, § 176.3 (2015); 18 PA. CONS. STAT. § 5705 (2015); R.I. GEN. LAWS § 11-35-24 (2015); S.C. CODE ANN. § 17-30-55 (West 2015); TEX. PENAL CODE ANN. § 16.02 (West 2015); UTAH CODE ANN. § 77-23a-5 (LexisNexis 2015); W. VA. CODE § 62-1D-4 (2015).

133. 18 PA. CONS. STAT. § 5705.

134. ME. STAT. tit. 15, § 710.

135. Press Release, Sen. Al Franken, After Pressure from Senator Franken, Federal Officials Take Action Against Dangerous “Stalking Apps” (Sept. 30, 2014) (on file with author).

136. CAL. PENAL CODE § 637.7 (West 2015); *see also* DEL. CODE ANN. tit. 11, § 1335(a)(8); TEX. PENAL CODE ANN. § 16.06.

it) likely has no application to cyber stalking apps because it only covers electronic tracking devices “attached” to a vehicle or movable thing.¹³⁷

We have seen some prosecutions of individuals responsible for the production of devices primarily designed to facilitate the stealth interception of communications. At the federal level, the owners of spy stores have been convicted of selling voice recorders and transmitters hidden in pens, light bulbs, wall plugs, and calculators.¹³⁸ Defendants have been imprisoned for selling wireless telephone microphones whose small size made them easy to hide and whose design permitted remote, clandestine monitoring.¹³⁹

Nonetheless, prosecutions remain extremely rare. Despite the increasing prevalence of spyware, federal prosecutors have only brought a handful of cases.¹⁴⁰ In 2005, a San Diego student, Carlos Perez-Melara, was indicted for manufacturing, selling, and advertising spyware programs called “EmailPI” and “Lover Spy.”¹⁴¹ The program was designed to “catch a cheating lover.” It sent victims an electronic greeting card that, once opened, would secretly install a keystroke logger and data-gleaning software. The program captured email, passwords, documents, and browser histories and sent reports of them to users on a regular basis. Users could take control of the watched person’s computer, including turning on the webcam and deleting or altering files.¹⁴² The case, however, fizzled after the defendant fled the country.

Nearly ten years elapsed before federal prosecutors charged another spyware producer under § 2512. In September 2014,

137. CAL. PENAL CODE § 637.7.

138. *United States v. Brio*, 143 F.3d 1421, 1430 (11th Cir. 1998); *United States v. Spy Factory, Inc.*, 951 F. Supp. 450, 476 (S.D.N.Y. 1977).

139. *United States v. Wynn*, 633 F. Supp. 595, 603 (C.D. Ill. 1986).

140. The first case involving spyware was brought in 1997 against Spy Shops International. The United States Attorney’s Office in Miami, with Assistant U.S. Attorney Robert Mosbacher in the lead, pursued § 2512 charges against the defendant for importing and selling spyware designed to be primarily used to intercept electronic communications surreptitiously. I am grateful to Robert Mosbacher for talking to me about the case.

141. China Martens, *‘Loverspy’ Creator Indicted, On the Run*, IDG NEWS SERVICE (Aug. 29, 2005).

142. *Id.*

federal prosecutors brought § 2512 charges against StealthGenie's CEO Hammad Akbar.¹⁴³ StealthGenie's spyware app secretly intercepted communications to and from mobile phones.¹⁴⁴ The company's marketing material explained that its app is "100% undetectable" and "runs in the background of the mobile phone without disturbing any of the other functions running."¹⁴⁵ StealthGenie promised to help subscribers "uncover the truth" by "secretly monitoring all the activities of your loved one or employee, and let you know their location at all times."¹⁴⁶ The federal indictment alleged that the app's target population was "spousal cheat: Husband/Wife or boyfriend/girlfriend suspecting their other half of cheating or any other suspicious behavior or if they just want to monitor them."¹⁴⁷ A federal judge issued a temporary restraining order authorizing the FBI to disable the site hosting StealthGenie.¹⁴⁸

Law enforcement has been slow to prosecute the distributors of spyware despite their life-threatening implications and illegal nature.¹⁴⁹ At the state level, criminal law's enforcement has been virtually nonexistent.¹⁵⁰ Why so few state and federal prosecutions?

One reason for the low number of prosecutions may be the difficulty in proving that a device is *primarily* designed for the secret interception of electronic communications.¹⁵¹ Privacy

143. Press Release, Fed. Bureau of Investigation, Pakistani Man Indicted for Selling StealthGenie Spyware App (Sept. 29, 2014) (on file with the author).

144. *Id.* Federal prosecutors in the Eastern District of Virginia brought the case because StealthGenie is hosted by a data center in Ashburn, Virginia. *Id.*

145. *Id.*

146. *Id.*

147. Zetter, *supra* note 26.

148. *FBI Arrests StealthGenie Mobile Spyware App Maker, Disables Website*, FBI NEWS BLOG (Sept. 20, 2014, 3:00 PM), http://www.fbi.gov/news/news_blog/fbi-arrests-stealthgenie-spyware-app-maker-disables-site (last visited Sept. 20, 2015) (on file with the Washington and Lee Law Review).

149. Zetter, *supra* note 26.

150. My research assistants and I searched Westlaw and Lexis for state law cases involving the prosecution of providers of stealth spying equipment and could not find any.

151. See Dempsey, *supra* note 103, at 111 (arguing that "Congress should delete the word 'primarily,' at least as it affects manufacture, sale, assembly, and

advocate James Dempsey blames the small number of § 2512 prosecutions on the fact that it is hard to demonstrate that equipment is “primarily” designed for stealth interception of communications.¹⁵²

Another reason is that law enforcement generally devotes too few resources to combating domestic violence and stalking. State and local police departments receive little training about relevant laws and technologies. Law enforcement’s lackluster response is also related to the view that cyber stalking is no big deal.¹⁵³ Law enforcement officers often advise victims that they have more important matters to address, such as murder and child porn, and lack the resources for cyber stalking cases.¹⁵⁴

Additional problems include the fact that cyber stalking and domestic abuse are under-reported. Because victims do not think that law enforcement will take their complaints seriously, they often do not seek out its help.¹⁵⁵ There is also a significant lack of digital forensic resources resulting in proof problems for prosecutors.¹⁵⁶ Lastly, as has long been true, society has difficulty in quantifying the harm caused by privacy violations, which leads to failure by law enforcement to prioritize this type of enforcement.¹⁵⁷

advertisement”).

152. See *id.* (noting the difficulty in proving that a device that is capable of intercepting cellular and a range of other frequencies is “primarily useful” for the interception of wireless telephone conversations).

153. CITRON, *supra* note 30, at 185.

154. See Amanda Hess, *A Former FBI Agent on Why It’s So Hard to Prosecute Gamergate Trolls*, SLATE (Oct. 17, 2014, 4:23 PM), http://www.slate.com/blogs/xx_factor/2014/10/17/gamergate_threats_why_it_s_so_hard_to_prosecute_the_people_targeting_zoe.html (last visited June 20, 2015) (“Cases that posed a serious risk of physical harm or a significant loss of property were prioritized, as were threats to children.”) (on file with the Washington and Lee Law Review). Although law enforcement agencies often dismiss cyber stalking victims because they claim they are too busy investigating terrorism or murder, FBI statistics tell another story. From 2010–2013, the top three crimes pursued by the FBI involved aggravated assault, drug crimes, and larceny theft.

155. CITRON, *supra* note 30, at 183–84.

156. See, e.g., *supra* note 150 and accompanying text (explaining that a significant barrier to recovery in common law tort cases is courts’ refusal to recognize privacy harms as justiciable or cognizable in the absence of financial harm).

157. See, e.g., *id.* (noting that the author’s Westlaw and Lexis searches for

We cannot be sure of the precise reasons for the under-enforcement of criminal law. But we can confidently say that criminal law has been rarely used to punish the production of equipment that has little use beyond the stealth interception of communications data.

C. Consumer Protection Laws

What about consumer protection statutes? Under § 5(a) of the Federal Trade Commission Act, the FTC can seek injunctive or other equitable relief against companies engaging in unfair or deceptive acts or practices.¹⁵⁸ Acts are considered unfair if they cause or are likely to cause substantial injury that consumers cannot reasonably avoid and their countervailing benefits to consumers or competition does not outweigh the costs.¹⁵⁹

Under its § 5(a) authority, the FTC has brought charges against spyware and mobile app providers engaged in the surreptitious collection of communications data. In 2012, the FTC alleged that DesignerWare LLC, a company providing spyware to rent-to-own computer providers, engaged in unfair and deceptive practices. The company's software secretly logged a computer user's keystrokes, photographed anyone in view of the computer's webcam, and tracked the computer's geolocation.¹⁶⁰ In 2013, DesignerWare entered into a consent decree with the FTC, agreeing not to gather data from computers without giving clear and prominent notice of such tracking at the time the computer is rented and without obtaining affirmative express consent.¹⁶¹

state law cases involving the prosecution of providers of stealth spying equipment produced no results).

158. 15 U.S.C. § 45(l) (2012).

159. *Id.* § 45(n).

160. Complaint, *In re* Matter of DesignerWare, LLC (2013), *available at* <https://www.ftc.gov/sites/default/files/documents/cases/2013/04/130415designerwarecmpt.pdf>.

161. Decision and Order, *In re* Matter of DesignerWare, LLC (2013), *available at* <https://www.ftc.gov/sites/default/files/documents/cases/2013/04/130415designerwaredo.pdf>.

Similarly, in 2008, the FTC brought a suit against CyberSpy Software, which sold a keylogger program called RemoteSpy.¹⁶² RemoteSpy could be disguised as an innocuous attachment to an email. Once an email recipient clicked on the attachment, the program would be installed onto the recipient's computer. The spyware generated records of all of the keystrokes typed, images captured, passwords provided, and sites visited on the infected computers. To access the information intercepted and gathered by the spyware, users would log into a site maintained by the defendants.¹⁶³ CyberSpy Software urged its users to employ stealth email services to send the software so recipients could not identify them.¹⁶⁴

In 2010, CyberSpy entered into a consent decree with the FTC, in which it agreed to refrain from promoting, selling, or distributing software that would be installed on computers without the knowledge and express consent of the computers' owners.¹⁶⁵ The defendant agreed to install a popup notice that clearly and prominently disclosed the function of the software to computer owners.¹⁶⁶ It also pledged to retain records about its customers, including names, addresses, phone numbers, email addresses, payments, and items purchased.¹⁶⁷

Beyond spyware, the FTC has signaled that apps collecting geolocation data owe special duties to users.¹⁶⁸ The FTC brought an action against a flashlight app developer for failing to notify users before the app was downloaded that their geolocation

162. Complaint for Permanent Injunction and Other Equitable Relief, FTC v. CyberSpy Software, LLC, No. 08-CV-01872 (M.D. Fla. Nov. 5, 2008).

163. Press Release, FTC, Spyware Seller Settles FTC Charges; Order Bars Marketing of Keylogger Spyware for Illegal Uses (June 2, 2010) (on file with the author).

164. Preliminary Injunctive Order, FTC v. CyberSpy Software LLC, No. 08-CV-01872 (M.D. Fla. Nov. 25, 2008).

165. Stipulated Final Order for Permanent Injunction, FTC v. CyberSpy Software, LLC, No. 08-CV-01872 (M.D. Fla. Apr. 22, 2010).

166. *Id.*

167. *Id.*

168. See Paul Ohm, *Sensitive Information*, 88 S. CAL. L. REV. (forthcoming 2015) (discussing the significant risk of privacy harm emanating from unprotected geolocation data and the need for new laws that account for the sensitivity of this kind of information).

information would be collected and shared with third parties.¹⁶⁹ The consent decree required the defendant to provide a separate notice and opt-in consent to consumers before collecting their geolocation information.¹⁷⁰ The consent decree's lesson was that consumers must be clearly notified about the collection and sharing of geolocation data, the reasons for the collection and sharing, and the identity of third parties with whom geolocation data will be shared.¹⁷¹

As Daniel Solove and Woodrow Hartzog have powerfully argued, the FTC has laid down common law principles for the protection of consumer privacy.¹⁷² FTC settlements in cases involving DesignerWare LLC, CyberSpy Software,¹⁷³ Aaron's Rental,¹⁷⁴ and Android Flashlight app¹⁷⁵ make clear the agency's

169. See Press Release, FTC, Android Flashlight App Developer Settles FTC Charges It Deceived Consumers (Dec. 5, 2013), <https://www.ftc.gov/news-events/press-releases/2013/12/android-flashlight-app-developer-settles-ftc-charges-it-deceived> (last visited Oct. 20, 2015) (noting the FTC's allegation that "the company's privacy policy deceptively failed to disclose that the app transmitted users' precise location and unique device identifier to third parties, including advertising networks") (on file with the Washington and Lee Law Review).

170. See *id.* ("The settlement also requires the defendants to provide a just-in-time disclosure that fully informs consumers when, how, and why their geolocation information is being collected, used and shared, and requires defendants to obtain consumers' affirmative express consent before doing so.").

171. See *id.* (stating that consumers should not be left in the dark about how their information is going to be used).

172. See generally Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2014) (contending that the "FTC's privacy jurisprudence is functionally equivalent to a body of common law," given its breadth and influence on regulation on information privacy in the United States).

173. Stipulated Final Order for Permanent Injunction, *FTC v. CyberSpy Software, LLC*, No. 08-CV-01872 (M.D. Fla. Apr. 22, 2010).

174. See *Aaron's Rent-to-Own Chain Settles FTC Charges that It Enabled Computer Spying by Franchisees*, FTC (Oct. 22, 2013), <http://www.ftc.gov/news-events/press-releases/2013/10/aarons-rent-own-chain-settles-ftc-charges-it-enabled-computer> (last visited Sept. 20, 2015) (noting that the retailer "agreed to settle FTC charges that it knowingly played a direct and vital role in its franchisees' installation and use of software on rental computers that secretly monitored consumers including by taking webcam pictures of them in their homes") (on file with the Washington and Lee Law Review).

175. *Android Flashlight App Developer Settles FTC Charges It Deceived Consumer*, FTC (Dec. 5, 2013), <http://www.ftc.gov/news-events/press-releases/2013/12/android-flashlight-app-developer-settles-ftc-charges-it-deceived>

view that spyware and mobile apps collecting communications and geolocation data should not operate without express consumer consent. The FTC, however, can only do so much given its limited resources and power. The agency cannot issue fines under § 5.¹⁷⁶ Only if companies violate settlement orders can the FTC pursue them for monetary penalties.¹⁷⁷

What about state Attorneys General and state consumer protection agencies? Under state unfair and deceptive trade practice acts, Attorneys General can seek civil penalties and injunctive relief against spyware app providers' unfair and deceptive consumer practices.¹⁷⁸ Unfortunately, far too little attention has been paid to the issue on the state level.

There are important exceptions.¹⁷⁹ The Attorney General of California, Kamala Harris, for instance, has been an aggressive advocate for online privacy.¹⁸⁰ She issued the guidance document "Privacy on the Go" with recommendations for mobile apps to

(last visited Sept. 20, 2015) (on file with the Washington and Lee Law Review).

176. See DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 854 (5th ed. 2014) (noting that there is no initial fining authority under § 5 of the FTC act).

177. If companies violate the terms of a final order issued by the FTC, then they could be liable for penalties up to \$16,000 per violation. 15 U.S.C. § 45(l) (2012).

178. See, e.g., CAL. BUS. & PROF. CODE § 17203 (noting that the provision allows for both monetary damages and injunctive relief in the case of unfair and deceptive consumer practices).

179. The Attorneys General of Florida, California, and Texas investigated Designerware for unfair and deceptive practice of secretly spying on computer renters.

180. See Jason M. Crawford, *State AGs and Online Privacy: Trends We Saw in 2013*, LAW360 (Dec. 6, 2013, 1:50 PM), <http://www.law360.com/articles/493366/state-ags-and-online-privacy-trends-we-saw-in-2013> (last visited on Sept. 20, 2015) (maintaining that Harris has been aggressive in advocating for online privacy on behalf of California consumers) (on file with the Washington and Lee Law Review); Divonne Smoyer & Aaron Lancaster, *State AGs: The Most Important Regulators in the US?*, THE PRIVACY ADVISOR (Nov. 26, 2013), <https://privacyassociation.org/news/a/state-ags-the-most-important-regulators-in-the-us/> (last visited on Sept. 20, 2015) (noting that with the support and encouragement of Attorney General Harris, California continues to lead other states in the field of data privacy protection) (on file with the Washington and Lee Law Review). Of late, state Attorneys General have made consumer privacy a priority including Connecticut, Maryland, Texas, New York, and others. *Id.*

safeguard consumer privacy.¹⁸¹ A prominent goal of the AG's study was the minimization of consumer surprise.¹⁸² AG Harris's report called upon mobile app providers to ensure just-in-time notice about the collection of personal information to reduce the unexpected collection of consumer data.¹⁸³ In 2012, AG Harris created a privacy enforcement task force, which has investigated mobile app developers for failing to inform users what personal information they were collecting.¹⁸⁴ California's eCrime Unit has pursued computer intrusion criminal prosecutions.¹⁸⁵

Much more should be done on the state level to combat stalking apps and their ilk.

IV. Next Steps

This Part lays out a plan of action. The first step focuses on potential legal reform. The second sketches out possibilities to enhance the enforcement of existing laws. The last calls for private efforts to combat cyber stalking apps.

181. KAMALA D. HARRIS, *PRIVACY ON THE GO: RECOMMENDATIONS FOR THE MOBILE ECOSYSTEM* (Jan. 2013).

182. *See id.* ("Recognizing that the legally required general privacy policy is not always the most effective way to get consumers' attention, *Privacy on the Go* recommends a 'surprise minimization' approach.").

183. *See id.* (recommending enhanced measures to supplement legally required privacy policy to alert users about company data practices, possibly provided through notices "delivered in context and just-in-time").

184. *See* Press Release, California Dep't of Justice, Attorney General Kamala D. Harris Notifies Mobile App Developers of Non-Compliance with California Privacy Law (Oct. 30, 2012) (noting that the letters are the first step in enforcing the California Online Privacy Protection Act, which "requires commercial operators of online services, including mobile and social apps, which collect personally identifiable information from Californians to conspicuously post a privacy policy") (on file with author).

185. For instance, California's Department of Justice prosecuted George Bronk for hacking into women's email and Facebook accounts to steal their nude photos. Bronk sent the nude photos to the women's email contacts. Nina Mandell, *Facebook Stalker Turned Email Hacker Sentenced to Four Years in Prison: Sent Nude Photos of Victims*, N.Y. DAILY NEWS (July 24, 2011), <http://www.nydailynews.com/news/national/facebook-stalker-years-prison-article-1.156894> (last visited Sept. 20, 2015) (on file with the Washington and Lee Law Review).

A. Updating the Law

Let's consider potential criminal law reforms. In 2014, Senator Al Franken proposed the Location Privacy Protection Act (LPPA).¹⁸⁶ The impetus behind the bill was the rise of cyber stalking apps and their enablement of domestic violence and stalking.¹⁸⁷ A section of the LPPA would extend § 2512's coverage to devices that collect geolocation information.¹⁸⁸ Congress and state lawmakers should adopt this proposal. National domestic violence groups, consumer advocacy groups, the FTC, and the Department of Justice support the extension of § 2512 to geolocation data, and for good reason, given the risks accompanying the disclosure of location data.¹⁸⁹

In addition, § 2512 and similar state laws should be broadened to cover devices whose design renders them "useful" for secret interception and collection of electronic, wire, and oral communications (and geolocation data). The more demanding "primarily useful" standard should be jettisoned as it erects an unnecessary barrier to criminal penalties.¹⁹⁰ Prosecutors may be reluctant to pursue § 2512 charges because it is hard to prove that their design renders them "primarily useful" for secret surveillance. The "primarily useful" standard allows defendants to point to a device's legitimate uses (e.g., parents keeping tabs on

186. Location Privacy Protection Act of 2014, S. 2171, 113th Cong. § 6 (2014).

187. *See id.* (proposing criminal penalties for "knowingly and willfully" disclosing geolocation information about an individual to another individual in aid of interstate domestic violence or stalking).

188. *See id.* (prohibiting development and distribution of stalking apps).

189. *See Location Privacy Protection Act of 2014: Hearing Before the Subcomm. on Privacy, Technology and the Law of the S. Comm. on the Judiciary*, 113th Cong. (June 4, 2014) (statements of Bea Hanson, Principal Deputy Dir., Department of Justice Office on Violence Against Women, and Jessica Rich, Dir., FTC Bureau of Consumer Protection) (expressing support for the extension of § 2512 to geolocation data given the unique risk that unknowing disclosure of such information poses for individual safety and privacy); Press Release, Senator Franken's 'Stalking Apps' Bill One Step Closer to Becoming Law (Dec. 13, 2012) (noting that Franken's bill "has been endorsed by nearly every national domestic violence and consumer group in the country").

190. *See* Dempsey, *supra* note 103, at 111 (outlining the difficulty in meeting the "primarily useful" standard and arguing for its eradication).

their children) as cover for its illegitimate ones.¹⁹¹ This tough standard has permitted spying businesses to flourish even as they market their spying software as “100% undetectable.”

Rather than the “primarily useful” standard, federal and state wiretapping statutes should cover the provision of devices “designed for” the stealth interception and collection of communications and geolocation data. What makes a device highly likely to invade privacy is its covert nature. We do not need proof that a tool’s design renders it “primarily useful” for stealth interception and collection to punish its provision. That a tool is designed to accomplish surveillance in an undetectable manner is what makes it illegitimate.¹⁹² It should be illegal to manufacture, sell, or advertise software designed to covertly intercept communications and location data.

Would eliminating the “primarily useful” requirement deter the production of devices with legitimate uses? Hardly. As NNEDV’s Cindy Southworth has argued, apps engaged in legitimate monitoring—such as the parent worried about a child’s location or the employer concerned about an employee’s misuse of her phone—need not disguise their presence.¹⁹³ A parent can locate a child if the cell phone’s app database shows that the location app

191. As Senator Franken explained at the Senate Privacy, Technology, and Law subcommittee hearing on the proposed Location Privacy Protection Act, a stalking ware provider focused its advertising on people who suspected their intimates of cheating. Once it became clear that his office was investigating stalking apps, the company changed its advertising to focus on uses by employers and parents. *Privacy Location Stalking Apps*, C-SPAN (June 4, 2014) <http://www.c-span.org/video/?319758-1/privacy-location-stalking-apps> (last visited Sept. 20, 2015) (on file with the Washington and Lee Law Review).

192. See Paul Ohm, *The Myth of the Superuser: Fear, Risk, and Harm Online*, 41 U.C. DAVIS L. REV. 1327, 1401 (2008) (comparing the DMCA to § 2512 and arguing that “[i]f one characteristic of a tool is especially pernicious and unlikely to be useful for widespread, legitimate use, a narrow law can be written criminalizing the creation or distribution of that tool”).

193. See Grant Gross, *Mobile Spying Apps Fuel Domestic Violence, U.S. Senator Says*, PC WORLD (June 4, 2014), http://www.pcworld.idg.com.au/article/546855/mobile_spying_apps_fuel_domestic_violence_us_senator_says/ (last visited on Sept. 20, 2015) (noting that with legitimate parental monitoring apps the child knows they are being monitored and there is no need for these apps to hide their presence on mobile phones) (on file with the Washington and Lee Law Review).

is running. The same is true for employers who want to check on employees' activities during work hours.

Also, apps that do not hide their presence would help ensure that employers themselves do not run afoul of wiretapping laws. Suppose that an employer owns the cell phones that it provides to employees. The employer loads spyware apps on the phones. In states with two-party consent wiretap laws, the employer is at risk for prosecution if employees using the phones talk to others on the phone without getting their consent to being monitored.¹⁹⁴

State lawmakers should consider adopting long-arm statutes that would enable courts to exercise personal jurisdiction over foreign app developers. One approach is to adopt a long-arm provision that permits prosecutors to pursue defendants whose software has harmed its citizens or whose services host data in the state.¹⁹⁵

If lawmakers decline to adopt criminal law reforms, lawmakers could consider imposing record-keeping requirements for spyware providers that know or have reason to know their software is used for secret surveillance. Sellers would be required to keep records of purchases, including detailed information about their users. We saw record-keeping requirements in the FTC's consent decree in the CyberSpy case. The FTC and state agencies should be given oversight over record-keeping requirements and the power to seek civil penalties against violators. Criminal penalties could follow if record-keeping requirements are ignored.¹⁹⁶

Record-keeping requirements could help deter criminal activity. Because providers would have to keep records about their

194. An employer's use of spyware would be legitimate under federal and most state wiretapping laws if the employer monitored the employee's phone with the express or implied consent of the employee. Such monitoring would be illegal in the twelve states that require all parties to a communication to consent to the interception. Ohm, *supra* note 192, at 1485. The states that require the consent of all parties to a communication are California, Connecticut, Florida, Illinois, Maryland, Massachusetts, Michigan, Montana, Nevada, New Hampshire, Pennsylvania, and Washington. *Id.* at 1486 n.379.

195. Thanks to Venus Johnson and Jeff Rabkin for talking to me about jurisdictional issues and potential reform efforts in California. At the federal level, prosecutors asserted their jurisdiction over the StealthGenie CEO on the company's hosting of data in Virginia.

196. A similar regulatory scheme applies to the pornography industry under 18 U.S.C. § 2257.

customers, their records would put them on notice that their equipment is being used for secret spying. Providers might adopt measures—such as having icons signaling the presence of apps—to immunize themselves from criminal liability. Individual perpetrators might think better of using software to spy on intimates because the threat of criminal penalty might seem real. Having to provide detailed information to providers about their identities might deter some wrongdoing.

Another potential reform is to give the FTC the power to pursue civil penalties against entities whose devices are designed to intercept private communications and location data without detection. In testifying in support of Senator Franken's Location Privacy Protection Act of 2014, the FTC's Chief of the Bureau of Consumer Protection pressed the bill's supporters to give the FTC the ability to enforce the civil penalty provision of the bill.¹⁹⁷ Civil penalties could serve as a potent deterrent to stalking app producers.¹⁹⁸

What about private rights of action? Under current law, parties who know that they have been spied upon likely cannot sue the companies that enable the privacy invasions.¹⁹⁹ A main barrier to recovery in common law tort cases is courts' refusal to recognize privacy harms as justiciable or cognizable in the absence of financial harm.²⁰⁰ State and federal lawmakers could overcome these problems by recognizing a statutory private right of action against entities providing, selling, and advertising devices designed to secretly intercept communications and location data.

197. *Location Privacy Protection Act of 2014: Hearing Before the Subcomm. on Privacy, Technology and the Law of the S. Comm. on the Judiciary*, 113th Cong. (June 4, 2014) (statement of Jessica Rich, Dir., FTC Bureau of Consumer Protection).

198. Legislative permission would lend democratic imprimatur to agency action. The FTC has faced criticism about its enforcement efforts under § 5(a) on the grounds that the unfair and deceptive practices statutory language fails to provide adequate notice to defendants of what constitutes appropriate behavior. *The Federal Trade Commission and its Section 5 Authority: Prosecutor, Judge, and Jury: Hearing Before the H. Comm. on Oversight and Government Reform*, 113th Cong. (July 24, 2014) (statement of Prof. Gerard M. Stegmaier).

199. See generally *Luis v. Zang*, 2013 WL 811816 (S.D. Ohio Mar. 5, 2013) (holding that 18 U.S.C. § 2520 did not provide a private right of action for § 2512 violations).

200. DANIEL J. SOLOVE, *UNDERSTANDING PRIVACY* (2008).

What about concerns that legal reform will impede innovation? The legal agenda proposed here is not designed to impede legitimate business practices. In our digital age, personal data is routinely collected, processed, and shared. Behavioral advertisers personalize ads based on online browsing habits.²⁰¹ Social networks amass reservoirs of personal data including user-provided location information and message histories.²⁰² These entities engage in these practices for commercial purposes, whether to sell advertising or to enhance user experiences, not for illegal ends. The FTC common law and best practices set forth by some state Attorneys General have set forth basic fair information practice principles, including notice and transparency for the collection, use, and sharing of consumer data. Such practices can proceed because consumers are given clear and prominent notice (or opt-in consent) before personal data is collected.

These commercial enterprises have little in common with businesses that enable individuals to spy on another person's private communications and location without detection.²⁰³ They sell tools that enable the continuous and secret tracking of a person's communications and location by private spies.²⁰⁴ Spying Incorporated is distinct from commercial practices that adhere to fair information practice principles, and so in turn are the civil and criminal penalties that attach to it.²⁰⁵

201. See Alexis C. Madrigal, *I'm Being Followed: How Google—and 104 Other Companies—Are Tracking Me on the Web*, THE ATLANTIC (Feb. 29, 2012), <http://www.theatlantic.com/technology/archive/2012/02/im-being-followed-how-google-151-and-104-other-companies-151-are-tracking-me-on-the-web/253758/> (last visited Sept. 20, 2015) (“They can offer targeted ads based on how users act (behavioral), who they are (demographic), where they live (geographic), and who they seem like online (lookalike), as well as something they call ‘social proximity.’”) (on file with the Washington and Lee Law Review).

202. See *id.* (noting that these companies amass this data with the stated purpose of delivering more relevant advertising to consumers that makes more money for companies).

203. See *supra* note 198 and accompanying text (noting that the former do not seemingly promote nefarious ends whereas the latter do).

204. See *supra* notes 191–192 and accompanying text (noting that the spying recorded keystrokes, images captured, passwords provided, sites visited on the infected computers, and other information).

205. See *supra* note 198 (noting that such applications can cause serious and tangible physical harm to individuals, and not simply just harm their privacy).

B. Enforcement Efforts

Without question, a legal agenda must be paired with support for law enforcement. Law enforcement needs access to digital forensic expertise and training.²⁰⁶ Police officers need to better understand the dangers of stalking apps, investigatory techniques, and available laws.²⁰⁷

In a world of limited resources, the difficulty is identifying additional funding sources. It is expensive to hire digital forensics experts for each and every local police force. One possibility is for localities to join together to allocate money for digital forensic resources. Local law enforcement agencies could share access to experts. Another potential source of funding is the monetary penalties stemming from convictions under § 2512 and similar state laws. To the extent that § 2512 and similar state laws are enforced, the fines collected from convicted defendants could be diverted to funding digital forensic specialists.

Another avenue to encourage enforcement is the mandatory collection of statistics about investigations and prosecutions of § 2512 and state laws. Mandatory reporting rules would help shine light on what law enforcement is and is not doing to combat cyber stalking app providers. Interested advocacy groups could bring publicity to gaps in enforcement, garnering the interest of elected officials including state Attorneys General and district attorneys.

C. Private Sector Solutions

To be sure, legislative reform may move slowly and the enforcement of existing criminal law may make only small advances. In the meanwhile, private sector providers should work on other innovative solutions.

Consider the efforts by Apple and Google to ensure end-to-end encryption of their devices to protect against unwarranted

interests).

206. See Hess, *supra* note 154 (noting that law enforcement must receive more training and direction on how to tackle the harms posed by spying technologies).

207. See *id.* (arguing that state and local police departments receive little training about relevant laws and emerging spying technologies).

governmental intrusion.²⁰⁸ Smart phone manufacturers and ISPs might extend their efforts to protect consumers' privacy to include the adoption of technologies that make it difficult to install undetectable spyware. There may indeed be consumer demand for such a move. We have seen public support for encrypted cell phones to resist the spying eyes of government.²⁰⁹ There may be strong consumer demand for devices that are not vulnerable to spyware.

V. Conclusion

The time to strike against stalking apps and their ilk is now. With the increasing adoption of biometric technologies, wearable monitors, and networked home devices, our cell phones will amass an unimaginably detailed record of our lives.²¹⁰ As spyware proliferates, stalkers, domestic abusers, and identity thieves will have access to those intimate reservoirs of our personal data. The consequences will be grave. We need to confront the issue with all potential tools, including criminal and civil penalties. The private sector can play its role as well, for the good of consumers and society.

208. See, e.g., Kevin Poulson, *Apple's iPhone Encryption Technology is a Godsend, Even if Cops Hate It*, WIRED (Oct. 8, 2014, 6:30 AM), <http://www.wired.com/2014/10/golden-key/> (last visited Sept. 20, 2015) ("With an eye to market demand, the company has taken a bold step to the side of privacy, making strong crypto the default for the wealth of personal information stored on the iPhone.") (on file with the Washington and Lee Law Review).

209. See *id.* (maintaining that these enhanced safety protocols are being driven by consumer demand).

210. See, e.g., *Riley v. California*, 134 S. Ct. 2473, 2494 (2014) ("Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans 'the privacies of life.'"); FTC Staff Report, *Mobile Privacy Disclosures*, <https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf>.

VI. Appendix

Exhibit A:

A screenshot of a Google search results page for the query "cell phone spy software". The search bar at the top contains the text "cell phone spy software" and a blue search button with a magnifying glass icon. Below the search bar, there are tabs for "Web", "Videos", "Shopping", "News", "Images", "More", and "Search tools". The "Web" tab is selected and highlighted with a red underline. Below the tabs, the search results are displayed. The first result is "Cell Phone Monitoring - webwatcher.com" with a yellow "Ad" label, a 4.4-star rating, and a description: "iPhone & Android Monitoring! Monitor Child/Employee Cell Phone 5 Minute Install · 24/7 Customer Service · 100% Undetectable Monitor Android Devices - Monitor iPhone or iPad". The second result is "Remote Cell Phone Spy \$27 - remotecellspy.com" with a yellow "Ad" label and a description: "Does Not Require Access To The Phone. Monitor Calls, Text & More.". The third result is "#1 Cell Phone Spy in 2014 - TeenSafe.com" with a yellow "Ad" label and a description: "View Kid's Text, GPS, & FB Messages 100% Effective - 100% Free to Try". The fourth result is "Cell Phone Spy Software Reviews | mSpy, MobiStealth ..." with a description: "There's something to think about, right? All parents want to their kids to be safe and sound without intruding into their lives too much. Here at ... mSpy - MobiStealth - SpyBubble - TopSpy". The fifth result is "Best Phone Spy Reviews: Best Phone Spy – Top 5 Cell ..." with a description: "www.bestphonespy.com/".

cell phone spy software

Web Videos Shopping News Images More Search tools

About 4,250,000 results (0.54 seconds)

Cell Phone Monitoring - webwatcher.com
Ad www.webwatcher.com/phone-monitoring
4.4 ★★★★★ rating for webwatcher.com
iPhone & Android Monitoring! Monitor Child/Employee **Cell Phone**
5 Minute Install · 24/7 Customer Service · 100% Undetectable
Monitor Android Devices - Monitor iPhone or iPad

Remote Cell Phone Spy \$27 - remotecellspy.com
Ad www.remotecellspy.com/
Does Not Require Access To The **Phone**. Monitor Calls, Text & More.

#1 Cell Phone Spy in 2014 - TeenSafe.com
Ad www.teensafe.com/
View Kid's Text, GPS, & FB Messages 100% Effective - 100% Free to Try

Cell Phone Spy Software Reviews | mSpy, MobiStealth ...
www.top10spysoftware.com/
There's something to think about, right? All parents want to their kids to be safe and sound without intruding into their lives too much. Here at ...
mSpy - MobiStealth - SpyBubble - TopSpy

Best Phone Spy Reviews: Best Phone Spy – Top 5 Cell ...
www.bestphonespy.com/

Exhibit B:

