Forthcoming Volume 72:3 of the WASHINGTON & LEE LAW REVIEW (2015)

SPYING INC.

Danielle Keats Citron*

The latest spying craze is the "stalking app." Once installed on someone's cell phone, the stalking app can provide continuous access to the person's calls, texts, snap chats, 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 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 prevent the installation of spyware.

INTRODUCTION

Private spying is a booming business. A rapidly growing sector of the spying 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]

* 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, Margaret Hu, Robert Mosbacher, Chris Slobogin, Cindy Southworth, Rachel Levinson-Waldman, and David Vladeck for their insights. I'm grateful to Jeffrey Rabkin for reading drafts with his expert eye as well as to Venus Johnson, Robert Morgester, and the rest of Attorney General Kamala Harris's Task Force on Cyber Exploitation for their helpful suggestions. The Georgetown-Maryland Privacy Working Group provided wonderful guidance. Cassie Mejias and Mariel Shutinya provided helpful research assistance. 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 and his team of editors were a huge help.

[1] Aarti Shahani, *Smartphones Are Used To Stalk, Control Domestic Violence Victims*, National Public Radio, September 15, 2014.

The "stalking app" is the private spy's current tool of choice.[2] Search "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 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*, 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."[6]

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 phones. In real time, subscribers can listen to a phone owner's calls and video chats; they can view their texts, photos, calendars, contacts, and browsing habits.[7] 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, "Bug their room: listen in on their phone's surroundings and listen in on what is really going on behind closed doors."[8]

A key selling point of stalking apps is their stealth nature.[9] Subscribers are assured that once they download the spyware app to someone's phone, the

---

[2] Cahal Milmo, *Exclusive: Abusers Using Spyware Apps to Monitor Partners Reaches 'Epidemic Proportions*,' INDEPENDENT (U.K.) (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.

[3] See Appendix, Exhibit A.

[4] *Location Privacy Protection Act of 2014: Hearing Before the Subcomm. on Privacy, Technology and the Law of the S. Judiciary Comm.*, 113th Cong. (June 4, 2014), Testimony of the Cindy Southworth, Vice Pres. of the National Network to End Domestic Violence on behalf of the Minnesota Coalition for Battered Women, *available at* http://www.judiciary.senate.gov/imo/media/doc/06-04-14SouthworthTestimony.pdf [hereinafter Southworth Testimony].

[5] *Id.*

[6] United States v. Jones, 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring).

[7] Saiyai Sakawee, *This App Lets Men with "Several Girlfriends" Spy on Their Significant Others' Every Move*, TECH IN ASIA (Dec. 11, 2013), https://www.techinasia.com/app-lets-men-several-girlfriends-spy-significant-others-move/.

[8] http://www.flexispy.com.

[9] *Id.*

phone owner will be unable to detect the spyware.[10] Stalking apps are advertised as "100% undetectable."[11] 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."[12] Cellphone Spying stresses: "What 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."[13] HelloSpy claims that its app "silently monitor[s] text messages, GPS locations, call details, photos, and social media activity." 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."[14]

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 *California v. Riley*, with access to someone's cell phone, a viewer can reconstruct the "sum of an individual's private life."[15]

Although providers often emphasize that parents and employers could use their apps to check on children and employees, stalkers and domestic abusers are their targeted audience.[16] National Network to End Domestic Violence's 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."[17]

---

[10] mSpyVIP, *Cell Phone Spy – mSpy Review*, YOUTUBE (Dec. 15, 2012), https://www.youtube.com/watch?v=YNbT0At4Tsg.
[11] Southworth Testimony, *supra* note.
[12] *Location Privacy Protection Act of 2014: Hearing Before the Subcomm. on Privacy, Technology and the Law of the S. Judiciary Comm.*, 113th Cong. (June 4, 2014), Opening Statement of Chairman Franken, *available at* http://www.judiciary.senate.gov/imo/media/doc/06-04-14FrankenStatement.pdf.
[13] *How Do Cell Spying Apps Work?,* CELLSPYINGHQ (Jan. 15, 2014), http://cellspyinghq.com/how-do-cell-spying-programs-work/.
[14] Southworth Testimony, *supra* note, at 19.
[15] California v. Riley, 134 S. Ct. 2473, 2489 (2014).
[16] See Appendix, Exhibit B.
[17] Press Release, National Network to End Domestic Violence, Senate Bill Would Ban Stalking Apps and Save Women's Lives (June 4, 2014), http://nnedv.org/news/4296-senate-bill-would-ban-stalking-apps-and-save-women-s-lives.html.

If one digs at all, it becomes clear that stealth surveillance of ex-intimates is a key goal.[18] Stalking apps are hailed as the "spy in [a cheating spouse's] pocket."[19] 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."[20] 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."[21] 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?"[22] 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."[23] mSpy emphasizes that its software app helps people catch cheating wives.[24]

Much of this activity is illegal. Intercepting electronic communications without at least one party's consent violates federal and state wiretap laws. In most states and at the federal level, cyber stalking is a crime.[25] 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

---

[18] 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. Kate Knibbs, *Smartphone Spying Startup Will Keep an Eye on NYC*, DAILY DOT (Feb. 27, 2014), http://www.dailydot.com/technology/mspy-goes-to-nyc/. In March 2014, mSpy's website demonstrated the service with a man tracking the communications and whereabouts of his wife and son. 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/.

[19] *Id.*

[20] FlexiSpy, http://www.flexispy.com. 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."

[21] Milmo, *supra* note.

[22] Stealth Genie Official, *StealthGenie - World's Most Powerful Cell Phone Spy Software*, YOUTUBE (July 31, 2013), http://www.youtube.com/watch?v=YycVKHOCp0M&list=UUi2qZEeLu4x7-eH70o52njQ

[23] Kim Zetter, *The Criminal Indictment that Could Finally Hit Spyware Makers Hard*, WIRED (Oct. 1, 2014), http://www.wired.com/2014/10/stealthgenie-indictment/.

[24] mSpyVIP, *supra* note.

[25] DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE 123-25 (2014).

devices for stalking apps.[26] 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.[27] Because both the law and the technology are not well understood, law enforcement does little beyond advising victims to get rid of their phones. Resources to fund digital forensic investigations are especially scarce at the state and local level. Then too, the lack of cooperation between jurisdictions may prevent the apprehension of stalkers.

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 to know that the design of the device renders it "primarily useful" for the covert interception of electronic, wire, or oral communications. Twenty-five states and the District of Columbia have similar criminal statutes. 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 the apps are "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 may 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, stalking app providers have paid little attention. Such services continue to proliferate; their ads brazenly appear online.

---

[26] *Location Privacy Protection Act of 2014: Hearing Before the Subcomm. on Privacy, Technology and the Law of the S. Judiciary Comm.*, 113th Cong. (June 4, 2014), Testimony of Detective Brian Hill, Criminal Investigations Division, Anoka County Sheriff's Office, *available at* http://www.judiciary.senate.gov/imo/media/doc/06-04-14HillTestimony.pdf [hereinafter Hill Testimony].

[27] DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE (2014). The Attorney General of California Kamala Harris has been working hard to address this problem in her state. I'm 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 Special Attorney General Jeffrey Rabkin (notes on file with author).

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 by their stalkers. New phones must be purchased and time spent devising new passwords and accounts.[28] 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, now and in the future.[29]

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.[30] That number surely understates the problem given the increasing adoption of cell phones and availability of stalking apps.[31] 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.[32] A 2014 study sponsored by Digital Trust found that more than 50 percent of abusive partners used spyware or some other form of electronic surveillance to stalk victims.[33] 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;[34] in 2014, the Department of Justice's Bea Hanson testified that 6.6 million people are stalked annually.[35]

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

---

[28] Hill Testimony, *supra* note, at XX.

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

[30] Katrina Baum, Shanna Catalano, Michael Rand, and Kristina Rose, Stalking Victimization in the United States, Bureau of Justice Statistics, Special Report No. NCJ 224527 (January 9, 2009), 8.

[31] 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.

[32] Southworth Testimony, *supra* note, at XX.

[33] Milmo, *supra* note.

[34] Baum, supra note, at 8.

[35] *Location Privacy Protection Act of 2014: Hearing Before the Subcomm. on Privacy, Technology and the Law of the S. Judiciary Comm.*, 113th Cong. (June 4, 2014), Testimony of Bea Hanson, Principal Deputy Dir., Department of Justice Office of Violence Against Women, *available at* http://www.judiciary.senate.gov/imo/media/doc/06-04-14HansonTestimony.pdf.

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?

A legal agenda should include legal reforms. Current criminal law may be too 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's 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 consumer protection agencies bring enforcement actions against spyware providers.

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.[36] We have proposed a right to quantitative 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.[37]

---

[36] David Gray & Danielle Keats Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62 (2013); David Gray & Danielle Keats Citron, *A Shattered Looking Glass: The Pitfalls and Potential of the Mosaic Theory of Fourth Amendment Privacy*, 14 N.C. J.L. & TECH. 381 (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. F. 262 (2013). *See also* Danielle Keats Citron & Frank Pasquale, *Network Accountability for the Domestic Surveillance State*, HASTINGS L.J. (2011).

[37] Danielle Keats Citron & Frank Pasquale, *The Scored Society*, WASH. L. REV. (2014); Danielle Keats Citron, *Mainstreaming Privacy Torts*, 99 CALIF. L. REV. 1805 (2011); Danielle Keats Citron, *The Privacy Implications of Deep Packet Inspection*, *in* DEEP PACKET INSPECTION: A COLLECTION OF ESSAYS BY INDUSTRY EXPERTS (Office of the Privacy Comm'r of Can. 2009), *available at* https://www.priv.gc.ca/information/research-recherche/2009/keats-citron_200903_e.asp;

Part I 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 II 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 III 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. It wraps up by addressing potential non-legal strategies.

I. THE PRIVATE SURVEILLANCE BUSINESS

A. *Evolution of the Spying Trade*

Human beings are inherently curious. Gossip has long been a common pastime.[38] Predictably then, as soon as telegraphs and telephones became available for purchase, so did devices designed to intercept confidential telephone and telegraph communications.[39] In the early 1900s, telephone wiretap devices were widely advertised and sold.[40] Businesses and individuals bought them to spy on competitors, employees, and spouses.[41]

Over time, spying tools grew in variety and sophistication.[42] In the 1940s and 1950s, mail order catalogs sold location trackers, spy cameras, bugging devices, radio pills, and tiny tape recorders.[43] Available for purchase were bugging devices hidden in martini olives, suitcase handles, earrings, and tie clasps. Miniature bugging devices could broadcast conversations to a receiver a block away.[44] Parabolic microphones could pick up voices without being placed on the premises.[45] Catalogs sought to avoid entanglement with the law

---

Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CAL. L. REV. 241 (2007).

[38] DANIEL J. SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET (2007).

[39] SAMUEL DASH, THE INTRUDERS: UNREASONABLE SEARCHES AND SEIZURES FROM KING JOHN TO JOHN ASHCROFT 79 (2004). 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.*

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

[41] *Id.*

[42] DASH, *supra* note, at 85; *see also* Berger v. New York, 388 U.S. 41, 47 (1967).

[43] ALAN WESTIN, PRIVACY AND FREEDOM 90, 98 (1967).

[44] MYRON BRENTON, THE PRIVACY INVADERS 152 (1964).

[45] *Berger*, 388 U.S. at 47.

by warning buyers to use bugging tools "according to the laws of your community."[46]

The low cost of spying devices fueled their widespread adoption.[47] Businesses installed microphones in the walls of employee restrooms and desks.[48] Model homes and car salesrooms were equipped with hidden bugs to allow salespeople to overhear the musings of prospective buyers.[49] Husbands bugged their wives' bedrooms and wiretapped their home phones, and wives wiretapped and bugged their husbands' offices.[50]

Early bugging devices faced objections and legal restrictions. As the next Part 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 totalizing picture of someone's daily 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, snap chats, videos, and more. 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. Stalking apps generate a precise, comprehensive record of a cell phone owner's activities, communications, and location in real time. 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, snap chats, and location. The watcher can turn the person's phone into a bugging device and pick up their conversations.[51] Cell phone owners will have no reason to suspect the surveillance because spyware is designed to be undetectable.[52]

---

[46] BRENTON, *supra* note, at 155.
[47] To the tune of $250. *Id.* at 153.
[48] DASH, *supra* note, at 84.
[49] *Id.* at 85.
[50] *Id.*
[51] Knibbs, *supra* note.
[52] United States' Memorandum of Law in Support of Motion for Preliminary Injunction at 4, United States v. Hammad Akbar, Civil No. 1:14 CV 1273 (E.D. Va. Oct. 2, 2014).

In the near future, far more information will be linked to mobile personal devices. Already on the market are fitness exercise 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.[53] Let's consider a few examples. mSpy, a UK 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 35 to 44 years old, and 53% live in the United States. Texans and Californians drive the most traffic to mSpy's website.[54] 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.[55]

Highster Mobile allows users to "secretly track and spy on virtually any cell phone quickly and easily completely undetected."[56] On YouTube, a Highster 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 correct."[57] A Highster-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 woman!!"[58] 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!!!"[59] YouTube users reviewing the app said it is great to use to watch your "cheating spouse" or your kids.[60]

---

[53] Just to name just 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.

[54] Molly Mulshine, *Watch What You Text: iPhone Surveillance Startup Moves to NYC*, BETABEAT (Feb. 26, 2014), http://betabeat.com/2014/02/watch-what-you-text-iphone-surveillance-startup-moves-to-nyc/.

[55] Dickson, *supra* note.

[56] *Remote Cell Phone Tracker and Spy*, HIGHSTER MOBILE, http://www.highstermobi.com (last visited Jan. 21, 2015).

[57] louiseramirez88, *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.

[58] *Highster Mobile Reviews*, TOP 10 SPY SOFTWARE REVIEW, http://www.top10spysoftware.com/review/highstermobile.

[59] *Id.*

[60] 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.

C. *Perils of Spyware*

Spyware apps enable 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 who was living in Kansas.[61] Because her abuser had installed a cyber stalking app on her phone, her abuser knew that she had moved to Elgin, Illinois. He tracked her to a shelter and then a friend's home where he assaulted her and tried to strangle her.[62] 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 track down her and her children. The man murdered his two children.[63] In 2013, a California man, using a spyware app, tracked a woman to her friend's house and assaulted her.[64]

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 mobile devices have been providing their abuser with total access to every communication, search conducted, photo taken, book read on a reading app, snapchat shared, social network message received, activity on dating apps, and step taken—for days, weeks, and months. Victims have told law enforcement that they no longer feel comfortable using their phones for fear that their abuser has somehow reinstalled spyware on their phones. They can become paranoid about using networked technologies for work, socializing, and public conversations, lest their abuser track them down. They experience distress about being watched.[65]

That sort of chilling implicates our intellectual privacy.[66] 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 chilled in the face of unwanted monitoring.

---

[61] Franken Statement, *supra* note, at 2.
[62] *Id.*
[63] *Id.*
[64] Southworth Testimony, *supra* note, at 12.
[65] Studies have shown that people experience anxiety about being watched and misunderstood. Stuart A. Karabenick & John R. Knapp, *Effects of Computer Privacy on Help-Seeking*, 18 J. APPLIED. SOC. PSYCHOL. 461 (1988).
[66] NEIL M. RICHARDS, INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE (forthcoming 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).

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.[67] If victims lose their financial cushion, the harm that they experience will be far worse and their options more limited.[68]

II. LAW'S ROLE COMBATING SPYING INC.

> "Few threats to liberty exist . . . greater than that posed by . . . eavesdropping devices."[69]

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 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.[70] Telegraph wiretapping bans were soon extended to include wiretaps on telephones.[71]

The Supreme Court heard its first wiretapping case in 1928. In *Olmstead v. United States*, 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.[72] The Court reasoned that "projected voices" did not constitute "actual physical invasions" of the home warranting Fourth Amendment

---

[67] Preliminary Injunctive Order, Federal Trade Commission v. CyberSpy Software LLC, and Tracer R. Spence, No. 08-CV-01872 (M.D. Fla. Nov. 25, 2008), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2008/11/081128cyberspypi.pdf.
[68] Southworth Testimony, *supra* note, at 15.
[69] Berger v. New York, 388 U.S. 41, 63 (1967).
[70] *Id.* at 45-46.
[71] *Berger*, 388 U.S. at 45-46. California extended its prohibition of telegraph wiretapping to telephone wiretapping in 1905. DASH, *supra* note, at 81.
[72] *Olmstead*, 277 U.S. 438, 466 (1928).

protection. Because government agents cut into defendant's telephone wires outside his home and had not trespassed inside it, no Fourth Amendment violation had occurred, the Court held. That federal law enforcement had violated state wiretapping law was irrelevant.

As the Court noted in *Olmstead*, Congress could ban warrantless wiretaps to fill in the gaps left by the Constitution.[73] Federal lawmakers did just that in the Federal Communications Act of 1934. 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. The use of devices to secretly record face-to-face communications in private places was not banned.[74]

As a practical matter, the Communications Act offered scant protection against wiretapping. The Department of Justice interpreted Section 605 to mean that law enforcement could engage in wiretapping if it did not divulge material obtained via wiretaps to others.[75] 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 criminal charges against individuals when law enforcement engaged in the same activity.[76]

In 1967, two Supreme Court decisions—*Katz v. United States*[77] and *Berger v. New York*[78]—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. Under *Katz*, surveillance focused on the interception of a few conversations was constitutionally acceptable if the interception was approved

[73] 277 U.S. 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. 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." 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.

[74] DASH, *supra* note, at 83.

[75] Westin, *supra* note, at 177.

[76] Westin, *supra* note, at 179, 186.

[77] 389 U.S. 347 (1967).

[78] 388 U.S. 41 (1967).

by a judge and based on a special showing of need.[79] By contrast, lengthy, continuous, and indiscriminate electronic surveillance violated the Fourth Amendment.[80]

Katz involved an investigation of a man allegedly running an illegal betting operation. Agents listened to the man's calls by attaching a suction microphone to a telephone booth's roof. Katz was convicted based on evidence gathered by the microphone. The Court held that using a listening device to monitor telephone conversations in a public phone booth constituted a Fourth Amendment "search." In rejecting the trespass requirement, the Court declared that, "the Fourth Amendment protects people, not places."[81] The Court found that conversations in telephone booths 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.[82] The Court noted that phone booths function as spaces of aural repose.[83] 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]." Declining to extend Fourth Amendment protection would unsettle these broadly held expectations and raise the specter of a surveillance state.[84] 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."[85] 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.[86]

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.[87] Title III laid out a regime of protections "to compensate for the uniquely

---

[79] 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).
[80] 388 U.S. 41 (1967).
[81] 389 U.S. at 351.
[82] *Id*. at 351-52.
[83] *Id.*
[84] *Id*. at 354-59.
[85] *Berger*, 388 U.S. at 64.
[86] *Berger*, 388 U.S. at 47 (ruling wiretapping raised special Fourth Amendment concerns because it involved continuous intrusions, searches, and 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).
[87] 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.

intrusive aspects of electronic surveillance."[88] Law enforcement had to meet stringent warrant requirements to intercept telephone calls over the wires. 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.[89] Wiretap orders had to be narrowly tailored and time limited.[90] Officers had to "minimize" the interception of innocent conversations.[91] 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.[92] Wiretaps falling short of these requirements were banned.[93]

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

Private individuals engaged in secret wiretapping could face criminal charges. Under Title III, it is a felony to intercept electronic communications unless one of the parties to a communication consented to the interception.[94] In passing Title III, federal lawmakers 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 up the source of equipment highly useful for surveillance."[95] 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.[96] Defendants face fines of not more than $10,000 or imprisonment of not more than five years or both.

---

[88] Dempsey, *supra* note, 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).
[89] Kerr, *supra* note, at 380.
[90] *See* 18 U.S.C. § 2518(3), (5) (2012).
[91] 18 U.S.C. § 2518(5).
[92] Dempsey, *supra* note, at 70.
[93] For a thoughtful exploration of the significance of Title III and *Katz*, see Susan Freiwald, *A First Principles Approach of Communications' Privacy*, 2007 Stan. Tech. L. Rev. (2007).
[94] 18 U.S.C. § 2511 (2012). Most states follow this approach, though 12 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 Ill. L. Rev. 1417, 1485 (2009).
[95] S. REP. NO. 90-1097, at 2183 (1968).
[96] 18 U.S.C. § 2512(1)(b) (2012).

Section 2512 covers a "narrow category of devices whose *principal use* is likely to be for wiretapping or eavesdropping."[97] A surveillance device must be "sufficiently invasive or devious in purpose to warrant criminal prosecution."[98] The inquiry focuses on the degree to which a device's components render it useful for the secret interception of communications.[99] Disclaimers that customers should be advised of the law do not immunize defendants from conviction.[100] A defendant cannot avoid penalties under Section 2512 "by surrounding himself with disclaimers and closing his eyes to the [surreptitious] nature and use of the devices."[101]

Section 2512's safe harbor exempts entities that supply surveillance equipment to government agencies or communication providers.[102] For instance, the manufacture of network packet sniffers seemingly falls outside of Section 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 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.[103] Most state laws track the exact language of Section 2512, including its safe harbor provisions. Pennsylvania makes it a felony to intentionally

---

[97] 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. 1968 U.S. Code Cong. & Admin. News at 2112, 2184.

[98] *Shriver*, 989 F.2d at 906.

[99] United States v. Shriver, 989 F.2d 898, 906 (7th Cir. 1992). 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).

[100] United States v. Brio, 143 F.3d 1421, 1429 (11th Cir. 1998).

[101] United States v. Wynn, 633 F. Supp. 595, 606 (C.D. Ill. 1986).

[102] 18 U.S.C. § 2512(2)(a)(b) (2012).

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

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."[104] 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."[105]

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 explained and has worked to change, "there is no federal law banning the secret collection of location data."[106] 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."[107] This provision (and the few others like it) likely has no application to cyber stalking apps because it only covers electronic tracking devices "attached" to a vehicle or movable thing.[108]

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, spy stores have been convicted of selling voice recorders and transmitters hidden in pens, light bulbs, wall plugs, and calculators.[109] Defendants have been imprisoned for selling wireless telephone microphones whose small size made them easy to hide and whose design permitted remote, clandestine monitoring.[110]

Nonetheless, prosecutions remain extremely rare. Despite the increasing prevalence of spyware, federal prosecutors have only brought a handful of cases.[111] In 2005, a San Diego student, Carlos Perez-Melara, was indicted for

---

[104] 18 PA. CONS. STAT. ANN. § 5705 (West).
[105] ME. REV. STAT. tit. 15, § 710.
[106] Press Release, Sen. Al Franken, After Pressure from Senator Franken, Federal Officials Take Action Against Dangerous "Stalking Apps" (Sept. 30, 2014), http://www.franken.senate.gov/?p=press_release&id=2960.
[107] CAL. PENAL CODE § 637.7 (West); Del. Code Ann. Title 11, section 1335(a)(8); Tex. Penal Code Ann. 16.06.
[108] CAL. PENAL CODE § 637.7 (West).
[109] 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).
[110] United States v. Wynn, 633 F. Supp. 595, 603 (C.D. Ill. 1986).
[111] 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.

manufacturing, selling, and advertising spyware programs called "EmailPI" and "Lover Spy."[112] 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.[113] The case, however, fizzled after the defendant fled the country.

Nearly ten years elapsed before federal prosecutors charged another spyware producer under Section 2512. In September 2014, federal prosecutors brought Section 2512 charges against StealthGenie's CEO Hammad Akbar.[114] StealthGenie's spyware app secretly intercepted communications to and from mobile phones.[115] 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."[116] 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." [117] The federal indictment alleged that the app's target population was "spousal cheat: Husband/Wife of boyfriend/girlfriend suspecting their other half of cheating or any other suspicious behavior or if they just want to monitor them."[118] A federal judge issued a temporary restraining order authorizing the FBI to disable the site hosting StealthGenie.[119]

Law enforcement has been slow to prosecute the distributors of spyware despite their life-threatening implications and illegal nature.[120] At the state level, criminal law's enforcement has been virtually nonexistent.[121] Why so few state and federal prosecutions?

---

[112] China Martens, *'Loverspy' Creator Indicted, On the Run*, IDG NEWS SERVICE (Aug. 29, 2005).
[113] Martens, *supra* note.
[114] Press Release, Federal Bureau of Investigation, Pakistani Man Indicted for Selling StealthGenie Spyware App (Sept. 29, 2014).
[115] *Id.* Federal prosecutors in the Eastern District of Virginia brought the case because StealthGenie is hosted at a data center in Ashburn, Virginia. *Id.*
[116] *Id.*
[117] StealthGenie Official, *supra* note.
[118] Zetter, *supra* note.
[119] *FBI Arrests StealthGenie Mobile Spyware App Maker, Disables Website*, FBI NEWS BLOG (Sept. 20, 2014), http://www.fbi.gov/news/news_blog/fbi-arrests-stealthgenie-spyware-app-maker-disables-site.
[120] Zetter, *supra* note.
[121] 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.

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.[122] Esteemed privacy advocate James Dempsey blames the small number of Section 2512 prosecutions on the fact that it is hard to demonstrate that equipment is "primarily" designed for stealth interception of communications.[123]

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.[124] 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.[125]

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.[126] There is also a significant lack of digital forensic resources resulting in proof problems for prosecutors. 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.

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

Stalking app producers may be running afoul of consumer protection statutes. Under Section 5(a) of the Federal Trade Commission Act, the FTC can seek injunctive or other equitable relief against companies engaging in unfair

---

[122] Dempsey, *supra* note, at 111.
[123] Dempsey, *supra* note, at 111.
[124] CITRON, *supra* note, at 85.
[125] Amanda Hess, *A Former FBI Agent on Why It's So Hard to Prosecute Gamergate Trolls*, SLATE (Oct. 17, 1014), http://www.slate.com/blogs/xx_factor/2014/10/17/gamergate_threats_why_it_s_so_hard_to_prosecute_the_people_targeting_zoe.html. 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.
[126] CITRON, *supra* note, at 183-84.

or deceptive acts or practices. 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.[127]

Under its Section 5(a) authority, the FTC has brought charges against spyware and mobile apps 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.[128] 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.[129]

Similarly, in 2008, the FTC filed a suit against CyberSpy Software, which sold a keylogger program called RemoteSpy.[130] 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.[131] CyberSpy Software urged its users to employ stealth email services to send the software so recipients could not identify them.[132]

In 2010, the defendants entered into a consent decree with the FTC, in which they agreed to refrain from promoting, selling, or distributing software

---

[127] 15 U.S.C. § 43(n) (2012).

[128] https://www.ftc.gov/sites/default/files/documents/cases/2013/04/130415designerwarecmpt.pdf

[129] https://www.ftc.gov/sites/default/files/documents/cases/2013/04/130415designerwaredo.pdf.

[130] Complaint for Permanent Injunction and Other Equitable Relief, Federal Trade Commission v. CyberSpy Software, LLC, and Tracer R. Spence, No. 08-CV-01872 (M.D. Fla. Nov. 5, 2008).

[131] Press Release, Federal Trade Comm'n, Spyware Seller Settles FTC Charges; Order Bars Marketing of Keylogger Spyware for Illegal Uses (June 2, 2010), http://www.ftc.gov/news-events/press-releases/2010/06/spyware-seller-settles-ftc-charges-order-bars-marketing-keylogger.

[132] Preliminary Injunctive Order, Federal Trade Commission v. CyberSpy Software LLC, and Tracer R. Spence, No. 08-CV-01872 (M.D. Fla. Nov. 25, 2008).

that would be installed on computers without the knowledge and express consent of the computers' owners.[133] The defendants agreed to install a popup notice that clearly and prominently disclosed the function of the software to computer owners.[134] They also pledged to retain records about their customers, including names, addresses, phone numbers, email addresses, payments, and items purchased.[135]

Beyond spyware, the FTC has signaled that apps collecting geolocation data owe special duties to their users.[136] The FTC brought an action against a flashlight app developer for failing to notify users before the app was downloaded that their geolocation information would be collected and shared with third parties. The resulting consent decree required the defendant to provide a separate notice and opt-in consent to consumers before collecting geolocation information. The lesson to providers is 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.

As Daniel Solove and Woodrow Hartzog have powerfully argued, the FTC has laid down common law principles for the protection of consumer privacy.[137] FTC settlements in cases involving Designerware LLC, CyberSpy Software,[138] Aaron's Rental,[139] and Android Flashlight app[140] make clear the agency's view that spyware and mobile apps collecting communications and geolocation data should not operate without express consumer consent. The FTC, however, can take us only so far given its limited resources and power.

---

[133] Stipulated Final Order for Permanent Injunction, Federal Trade Commission v. CyberSpy Software LLC, and Tracer R. Spence, No. 08-CV-01872 (M.D. Fla. Apr. 22, 2010).
[134] *Id*.
[135] Stipulated Final Order for Permanent Injunction, Federal Trade Commission v. CyberSpy Software LLC, and Tracer R. Spence, No. 08-CV-01872 (M.D. Fla. Apr. 22, 2010).
[136] *See* Paul Ohm, *Sensitive Information*, 88 S. Cal. L. Rev. (forthcoming 2015).
[137] Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2014).
[138] Stipulated Final Order for Permanent Injunction, Federal Trade Commission v. CyberSpy Software LLC, and Tracer R. Spence, No. 08-CV-01872 (M.D. Fla. Apr. 22, 2010).
[139] Press Release, Federal Trade Comm'n, Aaron's Rent-to-Own Chain Settles FTC Charges that It Enabled Computer Spying by Franchisees (Oct. 22, 2013), http://www.ftc.gov/news-events/press-releases/2013/10/aarons-rent-own-chain-settles-ftc-charges-it-enabled-computer.
[140] Press Release, Federal Trade Comm'n, Android Flashlight App Developer Settles FTC Charges It Deceived Consumer (Dec. 5, 2013), http://www.ftc.gov/news-events/press-releases/2013/12/android-flashlight-app-developer-settles-ftc-charges-it-deceived.

The agency cannot issue fines under Section 5.[141] Only if companies violate settlement orders can the FTC pursue them for monetary penalties.[142]

What about state Attorneys General and state consumer protection agencies? Under state unfair consumer practice acts (often called little-FTC Acts), Attorneys General can seek civil penalties as well as injunctive relief against spyware app providers' unfair and deceptive consumer practices. Unfortunately, far too little attention has been paid to the issue on the state level.

There are important exceptions. The Attorney General of California Kamala Harris, for instance, has been an aggressive advocate for online privacy.[143] She issued the guidance document "Privacy on the Go" with recommendations for mobile apps to safeguard consumer privacy.[144] A prominent goal of the AG's study was the minimization of consumer surprise. 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.[145] In 2012, AG Harris created a privacy enforcement task force, which has filed enforcement actions against mobile app developers to inform users what personal information they were collecting.[146] California's eCrime Unit has pursued computer intrusion criminal prosecutions.[147]

---

[141] DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 854 (5th ed. 2014).
[142] 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. Section 5(l) of the FTC Act.
[143] Jason M. Crawford, *State AGs and Online Privacy: Trends We Saw in 2013*, LAW 360 (Dec. 6, 2013), http://www.law360.com/articles/493366/state-ags-and-online-privacy-trends-we-saw-in-2013; 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/. Of late, state Attorneys General have made consumer privacy a priority including Connecticut, Maryland, Texas, New York, and others.
[144] KAMALA D. HARRIS, PRIVACY ON THE GO: RECOMMENDATIONS FOR THE MOBILE ECOSYSTEM (Jan. 2013), *available at* http://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/privacy_on_the_go.pdf.
[145] *Id.*
[146] 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), https://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-notifies-mobile-app-developers-non-compliance.
[147] 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.

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

III. 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.

A. Updating the Law

Let's consider potential criminal law reforms. In 2014, Senator Al Franken proposed the Location Privacy Protection Act (LPPA). The impetus behind the bill was the rise of cyber stalking apps and their enablement of domestic violence and stalking. A section of the LPPA would extend Section 2512's coverage to devices that collect geolocation information.[148] 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 Section 2512 to geolocation data, and for good reason given the risks accompanying the disclosure of location data.[149]

Section 2512 and similar state laws also 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.[150] Prosecutors may be reluctant to pursue Section 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 their children) as cover for its illegitimate ones.[151] This

---

[148] Location Privacy Protection Act of 2014, S. 2171, 113th Cong. § 6 (2014) (prohibiting development and distribution of stalking apps).

[149] *Location Privacy Protection Act of 2014: Hearing Before the Subcomm. on Privacy, Technology and the Law of the S. Judiciary Comm.*, 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); Press Release, Senator Franken's 'Stalking Apps' Bill One Step Closer to Becoming Law (Dec. 13, 2012), https://www.franken.senate.gov/?p=hot_topic&id=2254.

[150] Dempsey, *supra* note, at 111.

[151] 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. http://www.c-span.org/video/?319758-1/privacy-location-stalking-apps.

tough standard has permitted spying businesses to flourish even if they market their spying software as "100% undetectable."

Rather than the "primarily userful" 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 and enable stalking 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.[152] 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.[153] A parent can locate a child if the cell phone's app database shows that the location app 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.[154]

---

[152] *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 Section 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").

[153] 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/.

[154] 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, 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.

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.[155]

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 are 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 not followed.[156]

Record-keeping requirements could help deter criminal activity. Because providers would have to keep records about their customers, their records would put them on notice that their equipment is primarily 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.[157] Civil penalties could serve as a potent deterrent to stalking app producers.[158]

---

[155] 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.

[156] A similar regulatory scheme applies to the pornography industry under 18 U.S.C. 2257.

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

[158] Legislative permission would lend democratic imprimatur to agency action. The FTC has faced criticism about its enforcement efforts under Section 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*,

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.[159] 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.[160] 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.

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. Social networks amass reservoirs of personal data including user-provided location information and message histories. 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 has set forth basic fair information practice principles, including notice and transparency for the collection, use, and sharing of consumer data. Such practices can and should proceed if consumers are given clear and prominent notice of these practices.

These commercial enterprises have little in common with businesses that enable domestic abusers to spy on another person's private communications and location without detection. They sell tools that enable the continuous and secret tracking of a person's communications and location by private spies. Spying Incorporated is distinct from commercial practices with beneficial, legitimate uses, and so in turn are the civil and criminal penalties that attach to it.

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 about existing law. Police officers need to better understand the dangers of stalking apps, investigatory techniques, and available laws.

113th Cong. (July 24, 2014) (statement of Prof. Gerard M. Stegmaier), *available at* http://oversight.house.gov/wp-content/uploads/2014/07/Stegmaier-Statement-7-24-FTC.pdf.

[159] Luis v. Zang, Nos. 1:11–cv–884, 1:12–cv–629 (S.D. Ohio Mar. 5, 2013), *available at* 2013 WL 811816 (holding that 18 U.S.C. § 2520 did not provide a private right of action for Section 2512 violations).

[160] DANIEL J. SOLOVE, UNDERSTANDING PRIVACY (2008).

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. Another is for localities to obtain funding from the Department of Justice. Local law enforcement agencies could share access to experts. Another potential source of funding is the monetary penalties stemming from convictions under Section 2512 and similar state laws. To the extent that Section 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 Section 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 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 near term. Private sector providers could help envision other solutions. Apple and Google are moving to end-to-end encryption to deal with governmental intrusion. Smartphone manufacturers and ISPs might adopt technologies to prevent the installation of spyware without the consent of the device owner. 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. There may be strong consumer demand for devices that are not vulnerable to spyware.

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 rich record of our lives. 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.

Appendix

Exhibit A:

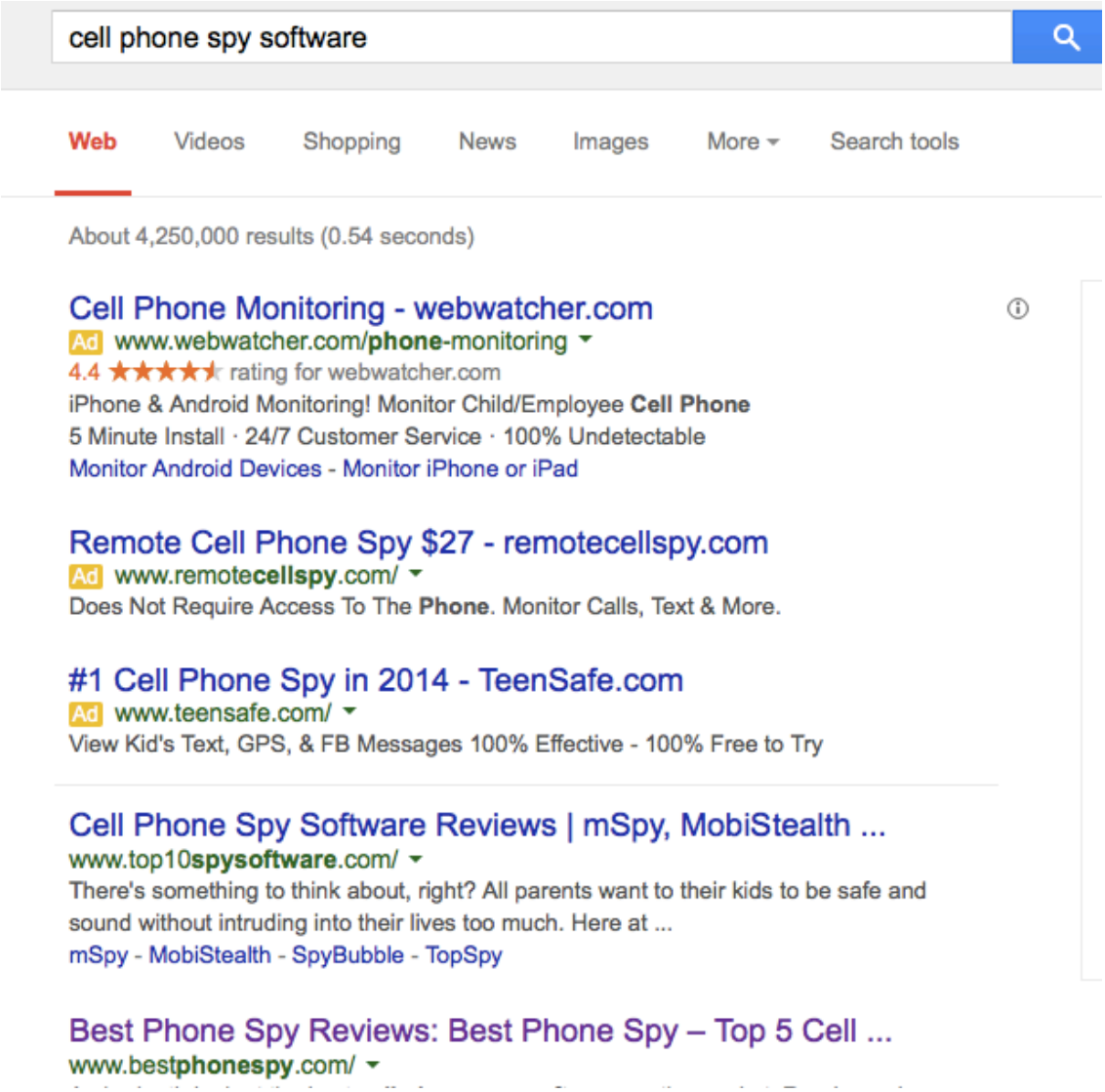
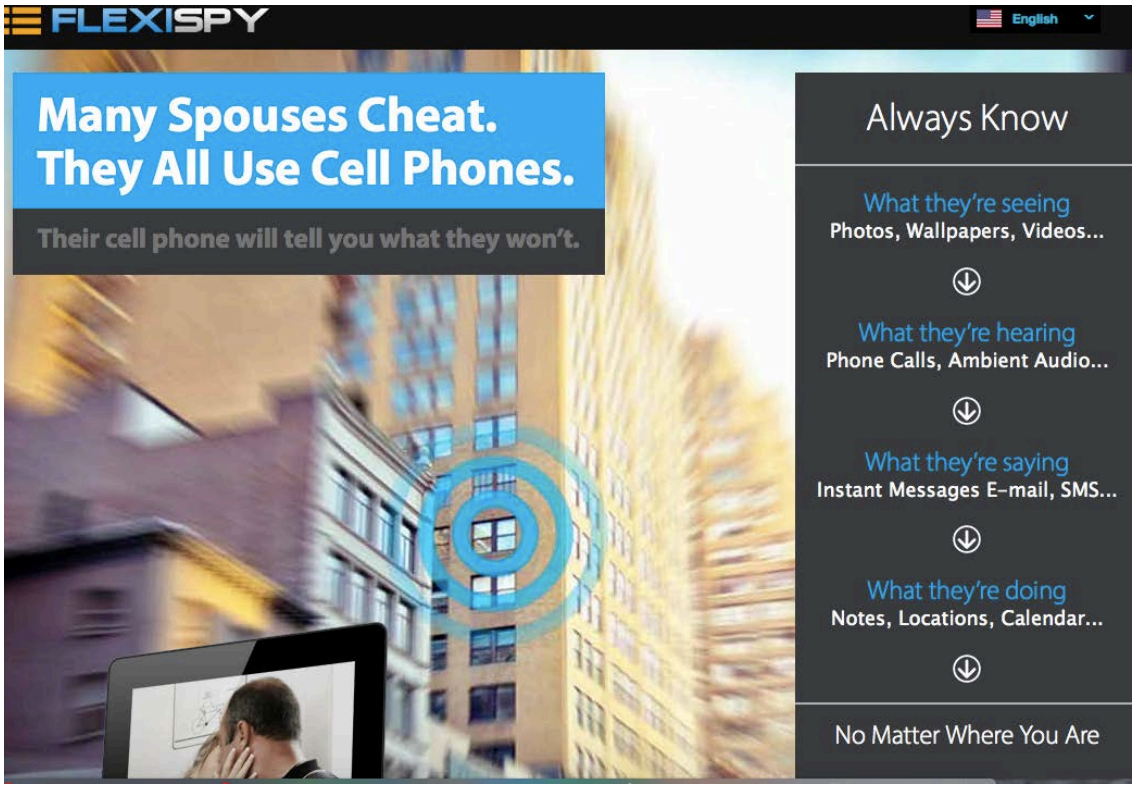


Exhibit B:


FLEXISPY
English
Many Spouses Cheat.
They All Use Cell Phones.
Their cell phone will tell you what they won't.
Always Know
What they're seeing
Photos, Wallpapers, Videos...
What they're hearing
Phone Calls, Ambient Audio...
What they're saying
Instant Messages E-mail, SMS...
What they're doing
Notes, Locations, Calendar...
No Matter Where You Are