

## **Interpartner Surveillance: Recent Developments in the Legal Response to Electronic Privacy Invasions**

### **Guilherme Roschke**

*Guilherme Roschke is a staff attorney at the ABA Commission on Domestic Violence where he provides technical assistance on electronic privacy and cyberlaw issues to domestic violence attorneys, as well working on the Commission's legal education programs. Prior to joining the Commission, Guilherme was a Skadden Fellow at the Electronic Privacy Information Center in Washington, DC. His fellowship focused on protecting the privacy of victims of domestic violence. Prior to law school Guilherme was a computer programmer with experience in corporate, non-profit and scientific environments. Guilherme is a member of the DC and NY bars. He received his JD from The George Washington University Law School.*

Relationships are the domain of the intimate, of the private. When relationships are abusive, this privacy is abused. Fortunately, some recent cases have affirmed the privacy interest of individuals in their intimate relationships. These cases improve the legal options for those victimized by tools widely available to perpetrators of domestic violence, harassment and stalking. Further, the Federal Trade Commission has for the first time taken action against a company marketing “Stalkerware” – spyware sold directly to consumers and marketed for uses such as spying on one’s spouse.

### **Technological Tools of Stalkers**

Hidden cameras and other surveillance technologies are available over the counter.<sup>1</sup> Bedside clocks or children’s toys contain hidden cameras – sometimes operating wirelessly. Computer spyware is commercially available, and marketed with claims such as how the software can “spy on anyone, from anywhere” and that it can “secretly and covertly” capture keystrokes, emails, passwords and more.<sup>2</sup> Some of these programs can be remotely deployed via an email attachment sent to the target computer. Some companies operate the surveillance as a service – the spy logs into the company website to read the reports on what the spyware has captured.

The effect of the widespread consumer availability of these technologies is that an individual without technical expertise can easily use these technologies for surveillance and cyber-harassment. On the other hand, lawyers will be able to find the evidence for these technologies in the business records of the companies, or in the credit card statements of the purchasers.

A recent report from the Department of Justice shows how common monitoring technologies were even few years ago.<sup>3</sup> The study covers victimization occurring mostly in 2005. An estimated 314,000 stalking and harassment victims experienced electronic monitoring.<sup>4</sup> Spyware was used in 44% of these cases, and video cameras, in 40%.<sup>5</sup> In addition, the report estimated 1.2 million victims of cyberstalking – via email, instant messaging, Internet websites and chat rooms.<sup>6</sup> It is likely that the numbers are even higher now, 4 years later, in 2009.

## The Legal Response to Surveillance

The range of surveillance activities can implicate several state and federal laws. Breaking into online accounts, such as email hosted at Hotmail or someone's social networking page may violate the Computer Fraud and Abuse Act.<sup>7</sup> A recent famous example of this is the hacking of the email account of former vice-presidential candidate Sarah Palin.<sup>8</sup> Tapping telephone lines or intercepting email communications violates the federal Wiretap Act.<sup>9</sup> However, some federal circuits have introduced inter-spousal immunities to federal wiretap law, with at least one being recently overturned. The Second Circuit has such an immunity;<sup>10</sup> the Fifth Circuit created an immunity,<sup>11</sup> but it was overturned in the Eleventh Circuit.<sup>12</sup>

Stalking laws may serve as a catch-all to various electronic monitoring techniques. The National Center for Victims of Crime Model Stalking Code states:

Any Person who purposefully engages in a course of conduct directed at a specific person and knows or should know that the course of conduct would cause a reasonable person to:

- (a) fear for his own safety or the safety of a third person; or
- (b) suffer other emotional distress,

is guilty of stalking.<sup>13</sup>

In a case of ongoing surveillance, an attorney should be able to meet the elements of this crime. The activity will be ongoing, and thus a 'course of conduct'. The surveillance will have a target, and thus be 'directed at a person'. The invasiveness of surveillance, and the exposure of personal details to an abuser or stalker will cause the requisite fear for safety and emotional distress. The challenge for attorneys will be to educate the court in the various technologies and techniques, and to lay the evidence for the harm experienced by the victim.

Finally, lawyers should be concerned with admissibility and ethical issues of surveillance. For example, the federal Wiretap Act provides an evidentiary exclusionary rule for intercepted aural communications, but not for electronic communications.<sup>14</sup> Thus illegally intercepted telephone communications cannot be introduced into evidence, but illegally intercepted emails and other non-aural communications can. However, in a Florida case interpreting a Florida statute modeled on the federal one, the court found intercepted electronic communications to be inadmissible.<sup>15</sup>

A client's or opposing party's use of surveillance technology may also raise significant ethical issues.<sup>16</sup> A client may wish to use spyware to detect evidence that will be helpful in the case. Or the client may share information with the

lawyer that was gained via questionable means, including communications that the other party has had with their lawyer. The lawyer should take note when the opposing party has spied on their client, and safeguard their communications with the client, including notifying the opposing attorney of their ethical duties.

## **Developments in the Legal Response to Spyware**

Last year, the Federal Trade Commission (FTC) filed its first case against a purveyor of consumer-grade spyware, or stalker spyware, called “CyberSpy”.<sup>17</sup> The case followed a complaint from the consumer group Electronic Privacy Information Center (EPIC).<sup>18</sup> In the complaint, EPIC alleged that several companies distributing spyware were engaged in unfair and deceptive trade practices under the FTC act. The EPIC complaint detailed the marketing activities of five purveyors of stalker spyware, the harms from spyware—including its use in domestic violence and stalking—and how consumer protection laws can be used to curb the marketing, distribution and operation of this software.

Previous FTC action on spyware had focused on companies that deployed spyware themselves, not providers of spyware to stalkers.<sup>19</sup> Only one previous similar case had been filed in 2005, when the creator and some users of the “LoverSpy” software were indicted by US Attorneys in California.<sup>20</sup> Among the distinguishing features between “Loverspy” and “CyberSpy” is that the former took care of all the details of the espionage, including infecting the computer to be spied upon.

The FTC action alleged that CyberSpy LLC sold the “RemoteSpy” software and (1) engaged in the unfair sale of spyware; (2) engaged in the unfair collection and disclosure of consumer information; (3) provided the means and instrumentalities to install spyware and access consumer’s personal information; and (4) provided the means and instrumentalities to engage in deception.<sup>21</sup> Per the FTC:

[T]he defendants provided RemoteSpy clients with detailed instructions explaining how to disguise the spyware as an innocuous file, such as a photo, attached to an email. When consumer victims clicked on the disguised file, the keylogger spyware silently installed in the background without the victims’ knowledge. This spyware recorded every keystroke typed on the victim’s computer (including passwords); captured images of the computer screen; and recorded Web sites visited. To access the information gathered and organized by the spyware, RemoteSpy clients would log into a Web site maintained by the defendants.<sup>22</sup>

The FTC complaint further details how the software was marketed, including promises of being “100% undetectable” with “stealth” and “cloaking” abilities. The FTC also points to the financial, health and safety harms that consumers are likely to experience when they are victimized by RemoteSpy users.

The CyberSpy case is ongoing. Its success would provide an example to other consumer protection authorities, such as state attorneys general or consumer lawyers, of a new tool to use in the fight against stalker spyware. Cyberspy LLC is not the only company providing this technology.

### **Developments in Video Surveillance**

Another invasive technique of intimate party surveillance is the use of video surveillance or video voyeurism technologies. The substantive legal questions raised in a claim against the abuser will usually turn on whether the victim had a “reasonable expectation of privacy.” Two recent cases show that state courts are taking a victim-friendly view of this concept.

In Iowa, a husband installed a video surveillance system in the marital home, consisting of a camera in an alarm clock and another in the headboard.<sup>23</sup> The wife requested tort damages in the divorce, claiming a violation of her privacy rights.<sup>24</sup> The husband, Jeffrey Tigges, claimed the wife, Cathy Tigges, had no reasonable expectation of privacy and that there were no damages because the tape was not published.<sup>25</sup> The record was unclear as to whether the recording took place while the parties shared the home. However, that fact did not matter to the court:

We conclude, however, the question of whether Jeffrey and Cathy were residing in the same dwelling at the time of Jeffrey's actions is not dispositive on this issue. Whether or not Jeffrey and Cathy were residing together in the dwelling at the time, we conclude Cathy had a reasonable expectation that her activities in the bedroom of the home were private when she was alone in that room. Cathy's expectation of privacy at such times is not rendered unreasonable by the fact Jeffrey was her spouse at the time in question, or by the fact that Jeffrey may have been living in the dwelling at that time.<sup>26</sup>

The court further noted that the cause of action for violation of privacy interest did not require the publication of the tape nor the actual taping of any compromising behavior.<sup>27</sup>

A Wisconsin case upholds an even stronger privacy interest in a scenario likely to be replicated by abusers. Unlike the *Tigges* case, the *Jahnke* matter concerned a felony violation. Mark Jahnke was convicted of secretly videotaping his girlfriend while she was nude in his presence.<sup>28</sup> Wisconsin law makes it a crime to record someone nude without their knowledge and consent, in a circumstance where they have a reasonable expectation of privacy.<sup>29</sup> Jahnke argued that when his girlfriend was naked in his presence, and in the view of his hidden camera setup, she did not have a reasonable expectation of privacy.<sup>30</sup>

The court instead agreed with the prosecution, that the proper test is whether the nude person had a reasonable expectation, under the circumstances, that they would not be recorded in the nude.<sup>31</sup> Though the videotape was made for private use, and not shared with others, the court still noted the importance of the privacy interest in preventing videotaping:

It is one thing to be viewed in the nude by a person at some point in time, but quite another to be recorded in the nude so that a recording exists that can be saved or distributed and viewed at a later time.<sup>32</sup>

## Conclusion

While new tools continue to be developed to aid perpetrators, and new technologies open new doors to survivors, the legal response must also remain dynamic. Common law doctrines such as the “expectation of privacy” have a place in the defense of victims of surveillance, and tools such as consumer protection laws help to address the consumer distribution of perpetrator technology.

---

<sup>1</sup> See Electronic Privacy Information Center, *Personal Surveillance Technologies*, [http://epic.org/privacy/dv/personal\\_surveillance.html](http://epic.org/privacy/dv/personal_surveillance.html).

<sup>2</sup> See Electronic Privacy Information Center, *Complaint, Request for Investigation, Injunction and Other Relief*, Mar. 6, 2008, [http://epic.org/privacy/dv/spy\\_software.pdf](http://epic.org/privacy/dv/spy_software.pdf).

<sup>3</sup> Bureau of Justice Statistics, *Stalking Victimization in the United States*, NCJ 224527 (January 2009), <http://www.ojp.usdoj.gov/bjs/pub/pdf/svus.pdf>.

<sup>4</sup> *Id.* at 5.

<sup>5</sup> *Id.*

<sup>6</sup> *Id.*

<sup>7</sup> 18 § U.S.C. 1030.

<sup>8</sup> *Palin Hacker Indicted*, *The Smoking Gun*, Oct. 8, 2008, <http://www.thesmokinggun.com/archive/years/2008/1008081palin1.html>.

<sup>9</sup> 18 § U.S.C. 2511.

<sup>10</sup> See *Anonymous v. Anonymous*, 585 F.2d 677 (2nd Cir. 1977).

<sup>11</sup> See *Simpson v. Simpson*, 490 F.2d 806 (5th Cir. 1974).

<sup>12</sup> See *Glazner v. Glazner*, 347 F. 3d 1212 (11th Cir. 2003).

<sup>13</sup> National Center for Victims of Crime, *The Model Stalking Code Revisited*, 24 (2007), <http://www.ncvc.org/ncvc/AGP.Net/Components/documentViewer/Download.aspxnz?DocumentID=4182>.

<sup>14</sup> 18 U.S.C. 2518(10)(a).

<sup>15</sup> *O'Brien v. O'Brien*, 899 So. 2d 1133 (Fla. Dist. Ct. App.. 2005)

<sup>16</sup> Sharon D. Nelson and John W. Simek, *Muddy Waters: Spyware's Legal and Ethical Implications*, GPSolo, Jan./Feb. 2006, <http://www.abanet.org/genpractice/magazine/2006/jan-feb/spywarelegalethicalimplications.html>.

<sup>17</sup> Federal Trade Commission, *Court Orders Halt to Sale of Spyware*, Nov.17, 2008, <http://www.ftc.gov/opa/2008/11/cyberspy.shtm>.

<sup>18</sup> Electronic Privacy Information Center, *Complaint, Request for Investigation, Injunction and Other Relief*, Mar. 6, 2008, [http://epic.org/privacy/dv/spy\\_software.pdf](http://epic.org/privacy/dv/spy_software.pdf).

<sup>19</sup> Center for Democracy and Technology, *Spyware Enforcement*, June 2008, <http://www.cdt.org/privacy/spyware/enforcement.php>.

<sup>20</sup> Department of Justice, *Creator and Four Users of Loverspy Spyware Program Indicted*, Aug. 26, 2005, <http://www.cybercrime.gov/perezIndict.htm>.

---

<sup>21</sup> Complaint for Permanent Injunction and Other Relief, *Federal Trade Commission v. Cyberspy Software* (M.D.Fla. 2008).

<sup>22</sup> Federal Trade Commission, *Court Orders Halt to Sale of Spyware*, Nov. 17, 2008, <http://www.ftc.gov/opa/2008/11/cyberspy.shtm>.

<sup>23</sup> *In Re Marriage of Tigges*, 758 N.W. 2d 824, 825 (Iowa 2008).

<sup>24</sup> *Id.* at 826.

<sup>25</sup> *Id.*

<sup>26</sup> *Id.* at 827.

<sup>27</sup> *Id.* at 830.

<sup>28</sup> *State v. Jahnke*, 762 N.W. 2d 696 (Wis. Ct. App. 2008.)

<sup>29</sup> *Id.* at 697.

<sup>30</sup> *Id.* at 698.

<sup>31</sup> *Id.* at 699.

<sup>32</sup> *Id.* at 700.