Policy Brief 1 | May 2020

DUKE CYBER POLICY AND GENDER VIOLENCE INITIATIVE

HTTPS://SITES.DUKE.EDU/GENDERVIOLENCEPOLICY/

REGULATING STALKERWARE USE:

IN DOMESTIC VIOLENCE CASES AND IN THE FACE OF COVID-19

In this Policy Brief:

BACKGROUND

By Joanne Kim | May 2020

DUKE CPGVI

Duke's Cyber Policy and Gender Violence Initiative seeks to explore and challenge the ways digital systems affect survivors of gender-based violence. Using data-driven and policy approaches, we seek to examine how to mitigate the impact of technologies on the privacy of survivors. Currently, our efforts are directed at supporting victims through the COVID-19 crisis. Our current work falls into 3 broad streams: data analysis, law and policy solutions, and outreach.

This policy brief is a working document. Any feedback will be considered for the final publication in Fall 2020.

KEY TERMS/ORGANIZATIONS

- Stalkerware: "software, made available directly to individuals, that enables a remote user to monitor the activities on another user's device without that user's consent and without explicit, persistent notification to that user in order to intentionally or unintentionally facilitate intimate partner surveillance, harassment, abuse, stalking, and/or violence" (also called spouseware)
- Spyware: "software designed to gather data from a computer or other device and forward it to a third party without the consent or knowledge of the user" (i.e. child-monitoring apps)
- Cyberstalking: escalated online-creeping used to "harass someone online"
- Domestic Violence (DV): "a pattern of behaviors used by one partner to maintain power and control over another partner in an intimate relationship" (also called intimate partner violence (IPV), domestic abuse or relationship abuse)
- The Coalition Against Stalkerware (CAS): formed by the Electronic Frontier Foundation (EFF), Kaspersky, Operation Safe Escape and seven other organizations in November, 2019, in response to the growing production, marketing, and abuse of stalkerware in the U.S. and around the world
- National Network to End Domestic Violence (NNEDV): "social change organization dedicated to creating a social, political, and economic environment in which violence against women no longer exists"
- National Coalition Against Domestic Violence (NCADV): "lead, mobilize and raise our voices to support efforts that demand a change of conditions that lead to domestic violence such as patriarchy, privilege, racism, sexism, and classism"
- Electronic Frontier Foundation (EFF): "leading nonprofit organization defending civil liberties in the digital world"
- Dual-Use Apps: "designed for some legitimate use case(s), but can also be repurposed by an abuser because their functionality enables another person remote access to a device's sensors or data, without the user of the device's knowledge"

BACKGROUND

LEGAL GOVERNANCE

- Children's Online Privacy Protection Act (COPPA): "imposes certain requirements on operators of websites or online services directed to children under 13 years of age, and on operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age"
- Federal Trade Commission Act (FTC Act): "outlaws unfair methods of competition and unfair acts or practices that affect commerce"
- Electronic Communications Privacy Act (ECPA): "amended, protects wire, oral, and electronic communications while those communications are being made, are in transit, and when they are stored on computers"
- Computer Fraud and Abuse Act (CFAA): "prohibits accessing a computer without authorization, or in excess of authorization"
- Two-Party Consent Recording Laws: "require the consent of every party to a phone call or conversation in order to make the recording lawful"
- One-Party Consent Recording Laws: "Federal law permits recording telephone calls and in-person conversations with the consent of at least one of the parties"
- Violence Against Women Act (VAWA): "outlined grant programs to prevent violence against women and established a national domestic violence hotline"

EXECUTIVE SUMMARY

THE PROBLEM

Domestic violence (DV) victims are not only attacked physically but also face an increasing number of cyber threats and abuses. 75% of 70 surveyed DV shelters have encountered victims whose perpetrators utilized hidden mobile eavesdropping apps to carry out abuse. A national survey also showed that "46% of Americans admit to 'stalking' an ex or current partner online without their knowledge or consent" with "10% admitting to using an app to monitor an ex or current partner's text messages, phone calls, direct messages, emails and photos." The prevalence of stalkerware in regular consumer markets and DV cases is concerning. For example, Kaspersky, a cybersecurity and antivirus provider, reported a 373% increase in stalkerware implementation and attempts of installation between 2018 and 2019 in their products alone (as seen in Figure 1).

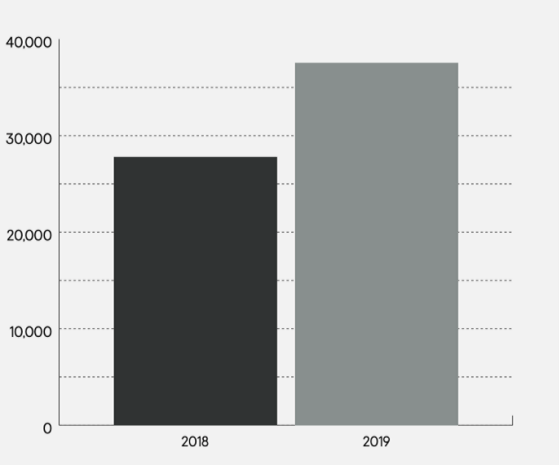


Figure 1. Users targeted by stalkerware 2018 vs. 2019

Enacted in light of COVID-19, social-distancing practices, stay-at-home orders, and quarantines have forced many DV victims to live under the constant surveillance of their abusers. "Abuse is being elevated and increased during this pandemic. They're taking away access to medicine and making sure survivors are isolated or intimidated," stated Rachel Gibson, Senior Technology Safety Specialist at the National Network to End Domestic Violence (NNEDV), in a private interview. Currently, local DV response lines are unable to handle the surge in phone calls, while Family Court can only accept 14% (12 out of 85) of its average number of cases pre-COVID-19.

Additionally, Eva Galperin, Director of Cybersecurity at the Electronic Frontier Foundation (EFF), commented that she expects an "uptick in stalkerware installation and use post-COVID-19" in a private interview. "We need to make it hard for abusers to access stalkerware right now," concluded Galperin.

Spyware companies also maintain low security measures which can lead to a breach of personal data and privacy. These companies also currently lack market transparency, as many continue to function as spyware and stalkerware providers.

RECOMMENDATION

Despite the dangers of stalkerware, there have been very limited policies, awareness, and research produced to effectively reduce the use of this technology. A strong short-term and long-term policy plan supported by the U.S. government, the Coalition Against Stalkerware (CAS) and its partners, and private sector companies is recommended to effectively regulate the spyware industry and limit the use of stalkerware.

WHAT IS STALKERWARE?

Stalkerware gives perpetrators complete access to a victim's digital properties, and in turn, allows abusers to assert more power and control over a victim's physical spaces. While all stalkerware is different, many give abusers the ability to "intercept calls; remotely switch on the device's microphone; monitor Facebook, WhatsApp, and iMessage chats; read text messages; track the phone's GPS location, and record the user's internet browsing history." Some also offer access to screenshotting capabilities, emails, and photo albums. Customers pay around $50 to $200 for monthly or annual subscriptions.

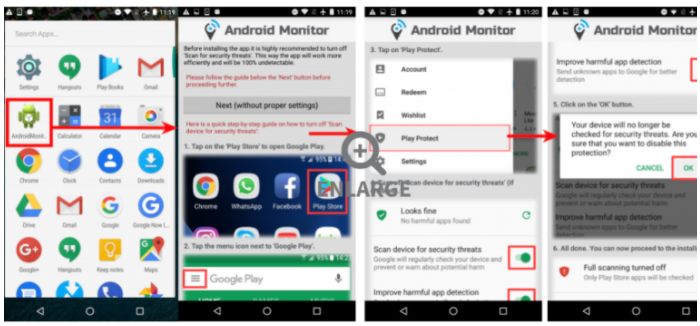


Figure 2. Stalkerware installation on an Android device
This particular software was disguised as an "Android Monitor." Once installed, the stalkerware "safeguards itself from Google's security framework."

Most stalkerware requires the abuser to have physical access to the victim's device for installation. According to Galperin, it is relatively easy for a perpetrator to obtain access to a victim's device, especially during a quarantine. Abusers often "shoulder-surf" for passwords, send links with malware, or demand access.

Once installed, the stalkerware runs in "stealth mode," providing no notification or identifying activity (as seen in Figure 2). Perpetrators then have the ability to monitor the device from a separate website or app, remotely.

According to Galperin, current computer crime laws, such as the Electronic Communications Privacy Act (ECPA), Computer Fraud & Abuse Act (CFAA), and state-level two-party-consent recording laws, apply to a substantial fraction of spyware company products. However, prosecution of stalkerware cases is nearly nonexistent and difficult for several reasons:

- U.S. Attorneys may not be interested in prosecuting charges of cyberstalking and online harassment due to the complexity of the cases.
- Federal agencies (i.e. FBI or FTC) "have jurisdictional limits to their investigations."
- Local law enforcement have a limited understanding of stalkerware and cannot collect strong evidence of cyberstalking.
- Victims are afraid to contact the police due to risk of escalating the situation.
- Many stalkerware apps are falsely marketed as "child or employee-monitoring" apps, which are legal under U.S. law.
- In Bernstein v. the U.S. Department of State, software source code was deemed speech protected by the First Amendment. Therefore, government regulations can not constitutionally limit the publication of spyware.

POLICY ISSUES

I. HUMAN RIGHTS

30% of all women and 16% of all men are affected by DV in the U.S. This means, that on average, "24 people per minute are victims of rape, physical violence, or stalking by an intimate partner." Furthermore, 60% of female victims and 40% of male victims "were stalked by a current or former intimate partner." Many victims do not escape and some die while trying. Approximately 760 people—more than two people per day—are murdered by their partners each year. Considered a public health concern by the NNEDV and Center for Disease Control and Prevention (CDC), DV is a persistent crisis that affects millions of Americans each year.

Stalkerware gives perpetrators more power and control and it has become a "standard part" of tormenting and stalking DV victims. Common cyberstalking tactics result in "unwanted phone calls, voice messages, and text messages from the perpetrator; the perpetrator showing up or approaching them in places, such as at home, school, or work, and being watched, followed, or spied on."

In a NPR survey, 85 % of the questioned shelters worked with victims whose abusers tracked them using GPS. Location-tracking abilities have made it especially harder for victims to escape their perpetrators and allow abusers to threaten victims' lives even after escaping their abusive homes. Furthermore, 50% of the shelters have a strict policy against using Facebook due to concerns that the abuser could utilize the pinpoint location function (see Figure 3 for full survey results). In general, shelters are increasingly focusing on "digital detoxes" to ensure that DV victims transition safely from their escape.

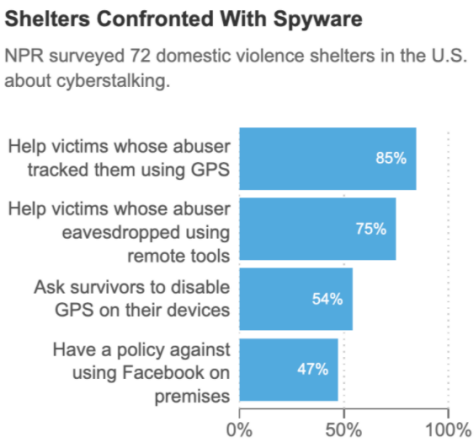


Figure 3. Shelters Confronted with Spyware

While the Violence Against Women Act (VAWA) and state DV laws legally protect victims, these cases are only brought to court after extensive physical, mental, and psychological abuse that results in years of trauma or permanent injuries. Therefore, it is critical to focus on preventative measures that will reduce the number of DV cases or at least minimize the trauma inflicted by such abuse. Regulating the commercial spyware industry and limiting the dangerous use of stalkerware in society is ultimately about restoring basic human rights - the "right to life, liberty, and the pursuit of happiness" - to 12 million+ annual DV American victims and survivors. It is imperative, especially during this time of social-isolation, to extend short-term and long-term help to DV victims.

II. DATA PRIVACY

DV victims abused by stalkerware are also at-risk of identity theft, financial extortion, and a basic infringement of personal privacy and data. Between 2017 and 2018, hackers were able to breach the data of eight spyware companies: FlexiSpy, Retina-X, TheTruthSpy, Mobisteath, Spy Master Pro, Spyfone, and SpyHuman. Several hackers have stated that the "companies' systems were not particularly difficult to breach." Since then, more hackers have exposed the low security measures of spyware companies. Cloud storage buckets set to public, exposed HTML code for back-end access, completely unprotected APIs, and leaving passwords on the internet were common privacy mishaps made by several spyware companies. L.M., a pseudonymous hacker, stated, "These companies take care about how to spy and don't care about victim's privacy or securing their data."

Photos of intimate moments, videos of children, audio recordings, contact information, text messages, browser history, and more are accessible either openly on the Internet or via simple data breaches (see Appendix A for possible list of breached data/intercepted data). Hackers warned that access to the stalkerware data also put the abuser at-risk of major financial extortion. Several customers "reused the same passwords for their email, PayPal, or Amazon accounts." According to hackers, the unprotected data could cost both the victim and the abuser. "It is very easy to ransomware them, and gain a lot of dirty money," said L.M.

In the FTCs first case against a spyware company, the Children's Online Privacy Protection Act (COPPA) and the Federal Trade Commission Act (FTC Act) were cited. The FTC found multiple violations of both COPPA and the FTC Act by Retina-X evident by "deceiving customers, broken security promises, repeated data breaches, user privacy invasions, and compromised device security." The case revealed the legal limitations of particularly the FTC Act and the lack of legislation on stalkerware in general. More regulation of the industry is necessary to protect the personal data of all involved parties and to prevent future identity and financial vulnerabilites.

III. MARKET TRANSPARENCY

Many spyware companies market their products as child or employee-monitoring software, positioning themselves as dual-use apps. In a private interview, Galperin stated, "If the tool is primarily used for covert surveillance then it's illegal. But, many stalkerware companies have changed the advertisement of their primary use." Furthermore, although app stores may remove stalkerware apps, many just rebrand themselves as "child-safety apps" and are reinstated.

Some spyware companies, such as FlexiSpy, still continue to "explicitly market its products to jealous lovers wanting to spy on their spouses. Illegal use cases for the malware are also advertised on multiple company social media accounts and websites (see Appendix B for stalkerware ad examples). The majority of stalkerware apps provide a wealth of resources that can "educate abusers about exploiting apps" for DV. In some cases, dual-use developers also encourage using the apps for DV "via advertisements, blogs, and customer support services."

Currently, anti-virus and anti-spyware tools "universally fail to identify dual-use apps as a threat." More research is needed to equip anti-virus companies with accurate detection tools and to regulate the spyware industry.

POLICY RECOMMENDATIONS

Duke's Cyber Policy and Gender Violence Initiative is open to adjusting and changing these recommendations. These are not completely developed and may change substantially in the final version. If you have any recommendations, please consider reaching out to the team.

GOVERNMENT

Short Term

- **Provide more financial assistance and resources during COVID-19.** Currently, the stimulus package - S.3548 - provides additional funding for the hotline, increases family services, provides unemployment aid, and etc., but it is still not enough. Galperin suggests that the government funds research for local DV shelters to assess what victims need at this time. Duke CPGVI recommends that more funding be allocated to DV shelters for running **an emergency version of the NNEDV's annual census project to figure out what services/resources shelters need and what help can be provided to victims.**

Long Term

- Propose a federal law that **mandates all states to enforce two-party consent recording practices.** 11 states already require that all parties involved must give consent before conversations/phone calls can be recorded. Passing this federal law will limit some of the abilities of an abuser utilizing stalkerware and also create cause for prosecution if perpetrators still choose to record their victims without consent.
- The Department of Justice should consider **internally encouraging Attorneys to take on more cyberstalking/online threat cases to provide justice to victims.** U.S. Attorney's offices only prosecuted 321 cybertstalking cases in 4 years. This number must be higher in order to restore justice to more victims.
- Local law enforcement offices should also consider teaching their officers how to mitigate stalkerware/cyberstalking cases. Duke CPGVI recommends **training workshops for current and incoming officers, especially since most DV cases are locally supported and reported.**

CAS & PARTNERS

Short Term

- CAS could partner with the NNEDV and National Coalition Against Domestic Violence (NCADV) to **research the impact of COVID-19 on stalkerware use**. The research could be used to better manage the distribution of the technology at this time.
- In a private interview, Gibson stated, "We need to train more people to be active bystanders. A grocery store employee could save a life." CAS could also partner with NNEDV, NCADV and reach out to hospitals, grocery stores, and pharmacies to inquire about **training staff on effective bystander practices.** Public education campaigns could also be run on major news outlets and radio stations. This will help connect more victims with the appropriate services during COVID-19.

Long Term

- CAS could partner with various organizations and institutions to both **conduct research and also build a digital library** for the public to easily access. Producing and providing research on stalkerware and DV will result in better-targeted resources and more informed decisions on the issue.
- CAS could **build up its digital education tools in partnership with NNEDV and NCADV.** Digital tools may include: public brochures on how stalkerware works and methods for removing it; robust virtual training sessions for people who want to volunteer at local response shelters; presentations and flyers that schools and universities can distribute to students.
- CAS could **work with more antivirus companies to model their software after Kapernsky.** Kapernsky was the first antivirus company to test and improve the accuracy of their dual-app/stalkerware detection tools.

POLICY RECOMMENDATIONS

PRIVATE SECTOR

Short Term

- Companies could **implement frequent internal checks to ensure that stalkerware apps are not available for download (i.e. on the Google Play Store) or being processed on their payment platforms (i.e. PayPal)**. As Galperin stated in a private interview, "We need to keep tech companies from enabling this abuse." It is recommended that companies designate specifically trained reviewers to spot stalkerware downloads or purchases. Duke CPGVI also recommends placing stricter restrictions on what apps can be sold or downloaded.
- Companies that sell ads could also check their ads to ensure that stalkerware is not being marketed. Google and Google-owned Youtube were two of the platforms which explicitly marketed stalkerware "to those hoping to spy on their spouses."Duke CPGVI recommends that other companies follow Google's response to these ads: **remove any stalkerware ads immediately and implement a more rigorous ad-reviewing process.**

Long Term

- Companies are recommended to **contribute to the limited DV/stalkerware research.** For example, Google published a study in response to finding stalkerware ads on their platforms and has promised to fund future studies.
- Spyware companies should **provide public transparency reports and administer "third-party assessments of their information security program every two years"** as recommended by the FTC . It is recognized that spyware companies which provide child and employee-monitoring software are legal; however, due to the dual-use nature of many spyware apps, Duke CPGVI recommends that companies become more transparent about the use of their apps.
- **Apple and Android could consider implementing a technical alert system that notifies users when their phones have been jailbroken or rooted** remotely**.** Jailbroken and rooted phones enable individuals to install unapproved third-party applications, such as stalkerware. Apple could alert a user if Cydia is installed on their device since Cydia is automatically downloaded when an iPhone is jailbroken. Similarly, Android devices could alert users if root managers (i.e. SuperSU, SuperUser, or Magisk Manager) are downloaded. Alerting DV victims when their devices have been jailbroken or rooted may enable them to become aware of the cyberstalking.

CONCLUSION

Stalkerware has become a standard part of DV cases, as perpetrators turn to digital spaces to assert more power and control over their victims. During this period of social-distancing, DV victims are trapped with their perpetrators for extended periods of time, and therefore, are more at-risk for escalated abuse. Under constant surveillance, victims will have a harder time escaping and will experience a greater infringement of privacy. In a private interview, Galperin suggested that stalkerware use will spike post-COVID-19 as abusers now have more opportunities to install the malware on the victim's device. Galperin also previously commented, "The apps have made it all too easy for domestic abusers and violent ex-partners to intimidate, threaten, and invade safe spaces of their targets, who are at risk of physical abuse." Measures must be taken to prevent stalkerware installations during this vulnerable time and restore basic human rights to DV victims.

The spyware industry is also highly at-risk for large data breaches and lacks market transparency. Both short-term and long-term measures enacted by the U.S. government's various branches, CAS and their partners, and private sector companies are necessary to effectively regulate the spyware industry and minimize the use of stalkerware by DV perpetrators.

APPENDIX A

DATA AVAILABLE IN BREACHES

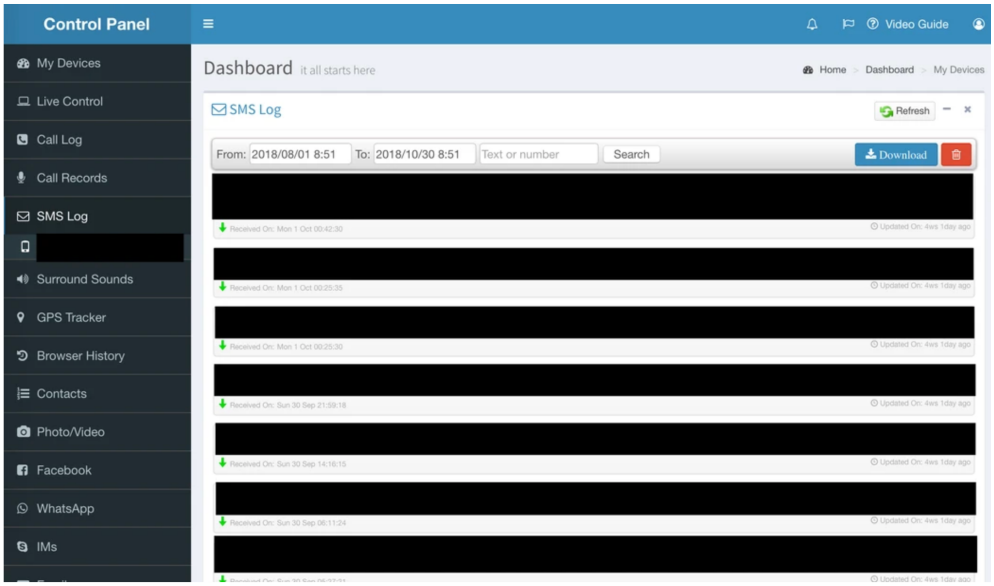


Image 1A. A screenshot of intercepted text messsages

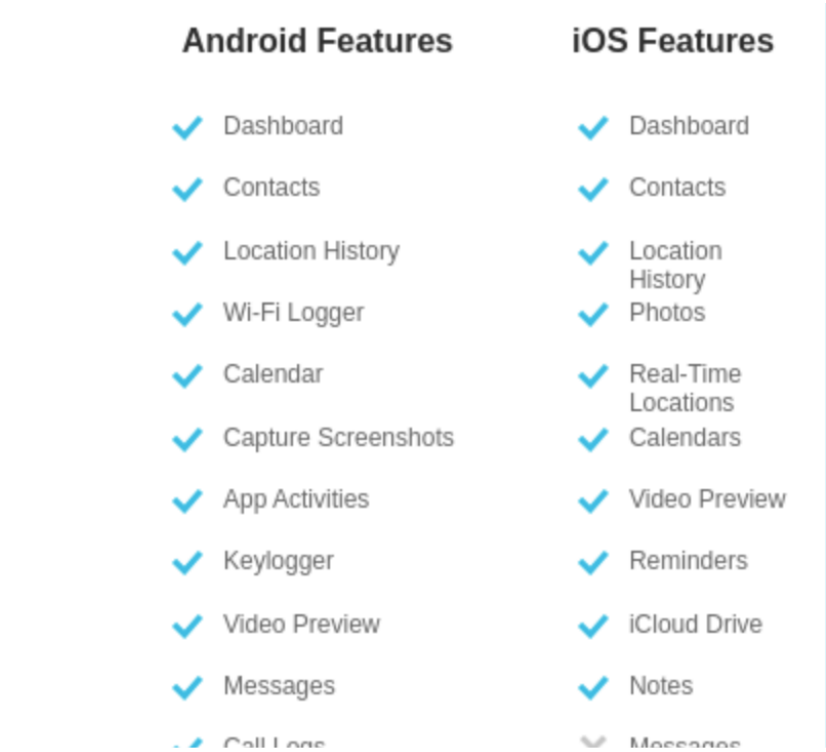
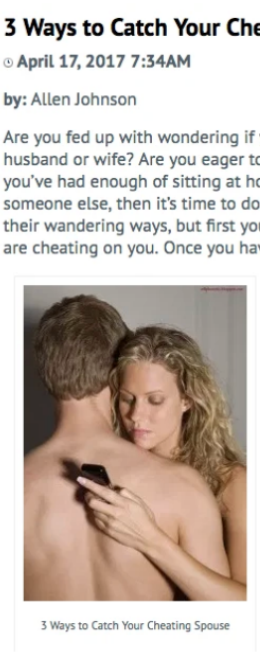


Image 2A. Data collected by spyware software and available in data breaches

APPENDIX B

STALKERWARE ADS



3 Ways to Catch Your Cheating Spouse

April 17, 2017 7:34AM

by: Allen Johnson

Are you fed up with wondering if you're being made a fool of by an unfaithful husband or wife? Are you eager to know how to catch your spouse cheating? If you've had enough of sitting at home fuming at the thought of your spouse with someone else, then it's time to do something about it. You don't have to put up with their wandering ways, but first you need to make absolutely certain that they really are cheating on you. Once you have solid proof, then let the confrontation begin.

3 Ways to Catch Your Cheating Spouse

[Image 1B. A screenshot of a blog post published by TheTruthSpy]

SPYMASTER PRO

CATEGORIES - HOT TAGS - SEARCH -

Spy on Your Partner's Phone This Valentine and Safeguard Your Relationship!

Admin | February 12, 2018 | no comments

Since, Valentine is round the corner, people are all set and enthusiastic to make this day a spectacular one and worth remembering. But, wait! This won't be the case with everyone! Who knows when you are preparing yourself for your big day your partner might be desperately looking for a newbie love.

So, what can be done? Well, just like you, there are many people around the globe who are unsure of their partner's loyalty and thus land up seeking help of a spy software. It has been seen that the demand of these softwares has constantly increased in recent years, as everyone wants to assure themselves whether their partner is cheating on them or not.

Popular Posts

CELL PHONE SPY How to Read my Girlfriend's Facebook Messages? July 19, 2014

CELL PHONE SPY How Can I Track My Wife's Mobile Phone Without Her Knowing? July 31, 2014

[Image 2B. SpyMaster Pro blog titled "Spy on Your Partner's Phone This Valentine and Safeguard Your Relationship"]

FlexiSPY
@FlexiSPYLtd

फ़ॉलो

Is FlexiSPY The Perfect Anti-Cheating App? #cheating #busted bit.ly/1WkFJnF

9:55 अपराह्न - 9 मई 2016

1

Thomas Brewster @iblametom · 10 मई 2016

@FlexiSPYLtd को जवाब दे रहे हैं

@FlexiSPYLtd Hey, any way I can speak to someone about Flexispy? Writing an article and includes info on the service.

[Image 3B. FlexiSPY tweet]