

Keep informed: Get the BetaBoston newsletters

X

THE ABUSE IN YOUR POCKET

As domestic abuse goes digital, shelters turn to counter-surveillance with Tor



George LeVines

@rhymeswthgeorge
2 HOURS AGO



1

Privacy



+2 More

Sarah's abuser gained access to every pass-

✉ GET BETABOSTON BY EMAIL

Your email address

Subscribe



Daily



Weekly highlights

Sign Up for My Beta



word she had. He monitored her bank accounts and used technology to abuse her location and read her conversations. She endured four years

of regular physical and emotional trauma enabled by meticulous digital surveillance and the existing support services, from shelters to police, were almost powerless to help her.

"We wish we could just stop the clock because we need to catch up," said Risa Mednick, director of the Cambridge domestic violence prevention organization Transition House.

To fight back, Transition House and others turn to the same methods used by intelligence agencies in order to keep their clients safe.

Sarah's case — one severe enough that using her real name would put both her and the domestic violence prevention community at risk — exemplifies how digital components of abuse stymie social workers more accustomed to dealing with physical and emotional trauma.

Mednick, whose organization worked with Sarah and others in similarly abusive relationships, saw first hand how her own staff struggled to handle casework involving technology. She responded by putting out a query for assistance.

Add tags to My
Beta to f
news stories,
trends, and



MY BETA

companies you
care about.

[CREATE AN ACCOUNT](#)

[LOGIN](#)

Already have **Boston.com** or
BostonGlobe.com account?
You can log in using your
existing credentials for
either site.

 **FOLLOW BETABOSTON**

[Follow @betaboston](#)

Last fall the Tor Project — a nonprofit that builds anonymous Web browsing and communication tools — answered Mednick's query. Since then, the two groups have been working to develop a resource that will provide staff and advocates with the base level of technological know-how required to address casework with a digital abuse component.

"Abuses with technology feel like you're carrying the abuser in your pocket. It's hard to turn off," said Kelley Misata, a Tor spokesperson.

The [Tor Browser Bundle](#) is free software that works like most ordinary browsers but comes configured to make it harder for individuals to be tracked, obscuring or deleting things like a browser's history, location, and IP address from both the website the user is browsing as well as erasing traces from the computer the browser is hosted on.

To better understand the dangers and the prevention community's response to digital abuse, I asked Transition House to connect me with one of their clients, someone who experienced total loss of control over their connected life.

Transition House introduced me to Sarah. She
needed to enter the
condition of anonymity. The domestic violence



prevention community expressed concern at the prospect of reaching out to her abuser or any member of his family, fearing retaliation both toward Sarah and Transition House.

Police reports and sworn affidavits, interviews with Sarah's family, her best friend, a current and former co-worker, and Transition House all corroborated Sarah's story.

BECOMING A PRISONER

Sarah and her abuser first struck up a relationship after meeting in a recreational soccer league in June of 2008. Things seemed to be going well after a weeklong vacation early on.

But two months in, after a brief breakup, he put her hands around her neck and threatened her life, Sarah said.

He blamed his behavior on a cocktail of drugs — some prescription, some not — to manage the long hours and stress incurred from what he told her was an undercover position at the Federal Bureau of Investigation.

The man insisted, citing the need to protect his

cover, that Sarah grant him access to every as-
set of her life: Google, e-mail, bank
accounts, website passwords. Everything.

**BetaBoston****MY BETA**

Feeling she had nothing to hide, Sarah com-
plied. That compliance soon evolved into a
complete relinquishing of freedoms.

Each day became the same: She went to work.
If she left a building she was to notify him. If she
didn't notify him, he called. When work ended
she went home. If she didn't go home, he called.

"The question I always asked was how does
someone end up in that situation?" her best
friend said. "And the answer — from having wit-
nessed it — is, gradually."

That gradual evolution is crucial to understand-
ing abuse, Mednick said.

Abuse works slowly: First abusers often forbid
Facebook, then friends of the opposite sex,
then friends altogether, then access to trans-
portation, then privacy of any kind. Without
noticing, a victim feels suddenly suffocated and
intensely vulnerable.

On New Year's Eve of 2008, Sarah's partner
passed out in their car after an argument over
the gratuity on their bar tab. She tried to help

him up the stairs but when he came-to he be-
can throw her against the wall, push her to the
ground, and finally kicking her into a wall before
passing out again.

"That night I was done with it," she said. "I felt like I couldn't talk to anybody because if I did, he would know. I felt more alone than I ever felt before. I was a prisoner in my own head because I couldn't tell anybody what was going on."

To escape, Sarah took about a hundred ibuprofen in an attempt to end her life.

TROUBLES WITH TECHNOLOGY

The first iPhone came out seven years ago. But for the law, those enforcing it, and providers of domestic violence prevention services, contemporary and pervasive use of Web and mobile computing technologies is still a challenge.

Sarah's case represents a larger trend, one where the lines blur between digital and real-life abuse. Most laws governing abuse and stalking came before the cell phone — and so do most social workers — making response to the trend challenging and slow.

"We're almost looking at Tor as technological epidemiologists," Mednick said.



The Cyber Crimes Division of the Mas-

sachusetts Attorney General's Office does not keep statistics specifically on cyberstalking. Nor does the Massachusetts District Attorney's Association. Even the Washington, D.C.-based National Network to End Domestic Violence (NNEDV) only managed to dig up a singular table generated by the National Institute of Justice — with data gathered in 2006.

"Unfortunately the most comprehensive statistics kept by the FBI don't drill down to that level of detail," said Cindy Southworth of NNEDV in an email.

Today, many abuse cases contain at least one digital facet because abuse is about power and control and most victims are using some form of technology, Southworth said.

Andrew Lewman, the Tor Project's executive director, understands better than most the challenges facing advocates and social workers in domestic violence prevention roles. Lewman works directly with abuse victims whose partners are in law enforcement or intelligence professions.

"You have a whole separate set of issues," he



The world Lewman works in looks especially grim. He sees abusers posting tips and tricks to online forums, telling others how to achieve masterful levels of surveillance and control.

A screenshot of the mSpy Blog website. At the top is a dark navigation bar with a logo and links: HOME, FEATURES, PRODUCTS, BUY NOW, COMPATIBILITY, HELP, ABOUT, CONTACT US. Below this is the 'mSpy Blog' title in purple. The main article is titled 'Spy on Girlfriend? mSpy Makes It Easy' in blue, dated 'July 6th, 2012 - Posted by admin'. The article features an image of a man in a suit with a brown paper bag for a head and dark sunglasses. The text describes mSpy as a mobile monitoring system that can track a girlfriend's phone, including call logs, text messages, and emails. It also mentions features like GPS tracking and the ability to read the address book. At the bottom of the article is a 'READ MORE' button and social media sharing links for Google+, Facebook, and Twitter, each with a '0' count.

For example, one abuser might hack a company's password database and share the whole thing with others online, Lewman said. Digital communities have sprung up where individuals teach each other how to compromise cell phones to track victim's whereabouts, listen to conversations in a room, take pictures, and read texts and email so that they can learn about

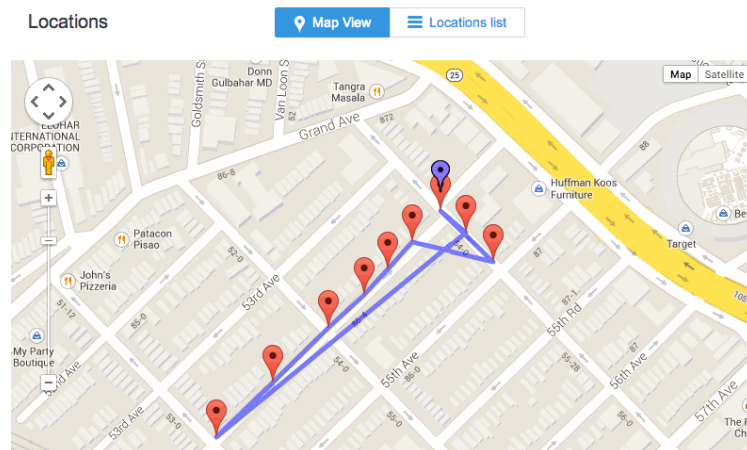
their victim's behavior on a microscopic level.

BetaBoston

Often the language to describe the surveillance

is couched in protective terms, such as moni-

toring a child's activities or queries posed to check if a partner is cheating. Commercially available software advertises easy tracking of exact locations, call logs, text messages, and more, often in an interface as easy to use as Google Maps.



And while digital stalkers often know nothing more about technology than the average person, their devotion is intense.

"Most of them quit their jobs and do this full time or they've been fired," Lewman said. "They spend all their time thinking about what they're going to do next."

In 2013 more than half of all US adults carried a smartphone according to the Pew Research

Center. To turn a device against someone, shelter workers need a certain amount of knowl-
edge and \$40. With a hacked phone an abuser

can track GPS location and gather exacting de-
tails through access to email, text messaging,
and other apps.

By contrast, in order to help victims in such a
predicament, social workers need a clear line of
communication, one insulated from abuser
snooping. Establishing that requires learning
the basics of encryption — a word many Ameri-
cans only became familiar with when stories
arose around the National Security Agency and
Edward Snowden.

"That's where Tor is useful because most social
workers are not tech savvy," said David Adams.
"We don't even know half the features on our
cell phones."

Adams is co-executive director at Emerge, an
organization founded in 1977 that runs educa-
tion programs for abusers, treating their actions
as learned behavior capable of being unlearned.

Emerge is developing a training module with
Lewman and Tor that both educates social
workers to be more aware of technological as-
pects of abuse and gives victims tools to "im-



munize" themselves, Adams said.



That project is still in the early phases. Lewman

first needs to understand how to teach social

workers to protect themselves before helping others. He thinks of the digital abuse epidemic like a doctor might consider a biological outbreak.

"Step one, do not infect yourself. Step two, do not infect others, especially your co-workers. Step three, help others," he said.

In the case of digital infections, like any other, skipping those first two steps can quickly turn caretakers into infected liabilities. For domestic violence prevention organizations that means ensuring their communication lines stay uncompromised. And that means establishing a base level of technology education for staff with generally little to no tech chops who might not understand the gravity of clean communication lines until faced with a situation where their own phone or email gets hacked.

While the Tor Project seeks funding to create a program that will give social workers that basic tech education, domestic violence advocates and victims remain in limbo when faced with challenging digital abuses.



AN INTERVENTION

**BetaBoston**

The overlords of digital protection held Sarah in the hospital, but she survived. Ultimately she and

her partner got back together.

It was 2010, two years into the relationship.

Sarah worked at a domestic violence shelter in Greater Boston. Every day she helped people in situations much like her own. She felt like a fraud.


"It was shoved in my face everyday," she said. "I didn't tell anybody what was going on."

Familiar patterns emerged. Sarah went to work and went home, notifying him of her every move. He called if she failed to do so. Slowly other staff at the domestic violence shelter learned about Sarah's situation.

She worried that he had weapons and the degree of stalking escalated to a point where she feared for her life.

Sarah's co-workers staged something of an intervention, sending her through a high-risk assessment team. The team acts to triage an abuse case and assess risk — including that of homicide — based on data points from law enforcement and service providers.

**MY BETA**

The communities of Cambridge, Arlington, and
 **BetaBoston**
bringing
together the Middlesex district attorney, law



enforcement, and domestic violence commu-
nity service providers from each town.

Surveillance within an abusive relationship
raises a red flag for an increased risk of homi-
cide, according to Adams, who wrote a book on
abusive men who murder.

The team assessed a very high risk to Sarah's
situation.

The domestic violence shelter she worked at
also worried about the integrity of its organiza-
tion and the services they provided because
Sarah's abuser knew of the shelter's location
and its business operations from information
he gleaned by surveilling her phone and Web
accounts.

The team developed an elaborate plan to pro-
cure a restraining order and get Sarah on a flight
out of state to stay with a trusted friend.

Obtaining a restraining order presented a num-
ber of complications, starting when Sarah's
partner drove by the courthouse, watching as
she walked up the stairs to file in early fall of

2010.



Filling out the paperwork, she feared he would

follow her into the courtroom. She knew him by

at least three different names seen on various identifications in his possession. She included all three in the restraining order. In the affidavit she explained the drive by that had just happened and detailed a number of past violent outbursts.

A local detective served Sarah's abuser the restraining order by phone. He called back that day to acknowledge the order.

Police decided to confiscate Sarah's smartphone in order to decipher whether it was in fact being used as a surveillance tool. They also decided she would be safer traveling by police cruiser to the airport rather than with a co-worker as the plan originally intended.

Sarah flew from Logan to stay with her best friend. Having complete access to her digital life, her partner knew exactly where she had gone.

"Before she got out here, I went out and bought a baseball bat and a couple cans of mace and prepared for the fact that he might follow her



out here," Sarah's best friend said.



The friend planned to provide a safe place for

her to relax and recover. Her plan and reality didn't line up.



"It set in pretty quick for me that she wasn't done with him," her friend said.

The friend found Google searches for pay phones in the area and assumed Sarah was trying to make contact with her partner. According to Sarah he had emailed her, violating the restraining order. She called to notify the domestic violence shelter of the violation.

In another email, Sarah's partner said that police had arrested one of his family members under the restraining order because the primary name that she knew him by — and one of the names she inscribed on the paperwork — in fact belonged to the family member.

Feeling guilty for putting the wrong person in jail, Sarah returned to the Boston area to release the family member and address threats he had made against her and her father.

"For me, for my friends, for my family, in that moment going back to him was the safest thing I could do," Sarah said.

RESTRAINT

≡ **BetaBoston**
For the domestic violence prevention commu-
nity, restraining orders are an important tool but



they come with a price. Victims and social workers devote hours and receive a token of moderate protection in return. Mednick calls the process an "endurance test" in which returning to the court over and over is not uncommon, often with the abusive person bringing their family and attorney, sitting directly across the aisle from the victim.

"It can feel very scary and you never know what's going to happen," Mednick said.

Scared is exactly how Sarah felt summer of 2012. She narrowly avoided being struck by a car when her partner shoved her into oncoming traffic after becoming angry with her for interacting with men at a gay bar.

She filed for a second restraining order later that week, court records show. The processing took far longer than with the first restraining order. From the Friday that she filed throughout the fall, she returned to the courthouse every 10 days in order to keep the order alive, five times in total.

In Massachusetts service of a restraining order

must occur in person unless a judge grants spe-
cific instructions on how to deliver the order of
delivery. For more than a month police tried

 **BetaBoston**



serving Sarah's partner to no avail. Eventually a judge granted the restraining order by allowing police to serve him via voicemail but warned Sarah that the order might not hold up should the defendant decide to fight it in court.

According to the affidavit she wrote and later recounted during an interview, it was only with the help of five strangers that Sarah managed to get in her car and leave the night he pushed her into oncoming traffic. In the affidavit she also revealed his supposed FBI cover and said she had not returned home after the incident for fear of seeing him.

Since obtaining that second restraining order Sarah has neither seen nor spoken to her former partner, except on one occasion when he saw her driving on U.S. I-93 and attempted to run her into a guardrail before exiting the highway.

HEALING

When Transition House staff learned about the courthouse drive by, the gravity of technological abuse struck.

"He knew to drive by a court that was com-
pletely unaware of my husband's mem-
ber with detailed knowledge of Sarah's case.

BetaBoston




Since then, response to digital abuse at some organizations has improved. Staff members ask questions to determine if cases contain a digital component earlier in the screening process. They are wary of client cell phones and compromised communication channels. If they feel a victim carries a bugged phone they replace it. If the abuse is happening across social media they encourage not using the platform in question.

However digital abuse often remains hidden until well after a victim's first contact with the organization, making it vulnerable to compromised communication lines, Mednick said.

In more severe cases the Tor Project gets involved and introduces some of their anonymizing tools to provide an added layer of security.

Meanwhile Sarah's restraining order remains precarious in the eyes of the law because it was served over voicemail. A court advocate told Sarah that her abuser was likely ducking the restraining order because there were warrants out for his arrest, she said. But when contacted

the Middlesex County Clerk's office said it found
the war on...
BetaBoston
... Sarah be-
lieved truly belonged to him.



Over the years Sarah's partner came to know and hold power over almost every detail of her life. In all she endured two lost jobs and two restraining orders. She was coerced into pregnancy and then miscarried. She survived monthly physical violence, persistent emotional trauma, and a suicide attempt.

More than a year out of the relationship — and lots of therapy later — Sarah said she still feels like she spent four years of her life with a person she knew absolutely nothing about. She eventually realized that he was likely not undercover FBI, but instead an abusive, married man with a drug habit.

"I had no idea who he was," Sarah said.

Six months after I first met with Sarah, she reflected on the struggle that started in June, 2008.

"No body is going to believe all of this stuff," Sarah said. "Even now I have a lot of shame. I have a lot of blaming myself."

After obtaining the second restraining order

she often called asking her best friend if partic-
ular social media posts were a sign of behavior
for which she received punishment for so long,

her best friend said.

"The entire thing was just such a surreal experi-
ence," said Sarah's friend. "It's a process, healing
— a long, never-ending process."

Sarah now works two jobs and is considering a
career change. She goes out with friends at
night and runs during the day. All things that she
could not or would not do for a very long time.

"I started playing soccer again," Sarah said.

[Typing image licensed from Shutterstock.](#)

*George is a regular contributor to BetaBoston, and can
be reached at george.levines@gmail.com. Follow
George on [Twitter](#) - [Google+](#)*



Learn more

Click "+" on any tag to track what matters to you.





LOG ON TO ADD YOUR COMMENT

Already have an account with
BostonGlobe.com or Boston.com?

Please log in using that info.

USE A SOCIAL NETWORK



TWITTER



FACEBOOK

OR YOUR BETABOSTON ACCOUNT

Cancel

Submit

[Need an account? Sign up here.](#)

[Forgot your password?](#)



Julian Cook

4 hours ago

A lot of people are just putting Tor on their PC/laptops thinking that they're instantly anonymous and they aren't. It's no secret that the U.S. and U.S. intelligence friendly countries

operate exit nodes expressly for the purpose of
facilitating government surveillance (that last hop is
unencrypted). Be wary of the browser bundle

 **BetaBoston**



from Tor. This bundle is the subject of special interest by U.S. authorities and they are constantly trying to exploit whatever version of Firefox that it uses and was recently successful (<http://arstechnica.com/security/2013/08/attackers-wield-firefox-exploit-to-uncloak-anonymous-tor-users/>). You could take the DIY route to be safe and just build a Tor router (powered by Linux) but you need to be a geek to do it or if you just want a fast solution get a PAPARouter (<http://paparouter.com>). It's inexpensive (less than \$100.00), allows you to anonymize several devices at once and best of all it excludes all U.S. and U.S. intelligence friendly exit nodes (over 50 at last count) built into it. Given all the uproar that other countries are having with U.S. spying (and rightfully so), making your last Tor relay outside of the U.S. to your target site is great security and using https would be massive protection by encrypting your data from that last hop to the target site. The Electronic Frontier Foundation has a great interactive page that demonstrates this. TOR AND HTTPS PAGE <https://www.eff.org/pages/tor-and-https>

SALES PITCH

These are the slides Digital Recognition Network uses to sell police and repo companies on its license plate surveillance database

Where does NVLS Data come from? Vigilant Video

Financial institutions are funding asset recovery programs by employing Licensed Fleet Operators (LFOs) that collect Vehicle Scan Records (VSRs).

LFOs drive pre-determined mapping routes scanning locations where vehicle assets are typically found to be candidates for recovery.

Vigilant Video's private LPR Network partner

Digital Recognition Network

(DRN - Forged by Vigilant Video)

Vigilant Video's Exclusive LPR Network Partner



Shawn Musgrave

@shawnmusgrave
03/11/2014



Last week, BetaBoston provided a glimpse into how a [handful of private data brokers have compiled massive databases of vehicle location records](#). By mounting high-speed license plate readers on tow trucks and repo "spotter" cars

in nationwide networks, these brokers claim to have connected scores of auto-theft vehicles registered in the United States. [READ MORE](#)

BetaBoston



Privacy



+3 More

PROTECTING BIG DATA

Former White House tech official has new privacy startup, TrustLayers



Scott Kirsner @ScottKirsner
03/10/2014



[Danny Weitzner](#), an MIT researcher who served as Deputy Chief Technology Officer at the White House under President Obama is hatching a new startup related to data privacy: [TrustLayers](#), which is out now raising a seed round of funding. Weitzner's co-founder is [Adam Towvim](#), a long-time executive at the mobile advertising startup Jumptap, [acquired last year](#) by Millennial Media. [READ MORE](#)

HANDS OFF MY BITS

Virgin Pulse fitness tracker is a case study in big data and privacy

 **Cal Borchers** @CallumBorchers
03/06/2014

This week's [White House/MIT Big Data and Privacy Conference](#) was pretty abstract. At least, it was for those of us who don't geek out over [homomorphic encryption](#). **READ MORE**

NOTHING TO SCAN HERE

Massive license plate location database just like Instagram, Digital Recognition Network insists



Shawn Musgrave

@shawnmusgrave
03/05/2014



1

At a state house hearing before the Massachusetts Joint Transportation Committee Wednesday afternoon, the chief executive of the largest license plate scan database in the country insisted that license plate recognition technology is "simply photography." **READ MORE**

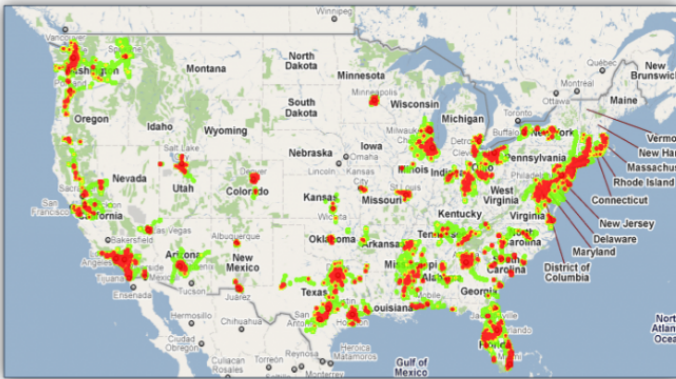
ALPR



+3 More

BIG DATA IS WATCHING

A vast hidden surveillance network runs across America, powered by the repo industry

LFO LPR Data Event Map – March 1st, 2010 through March 31st, 2010**Shawn Musgrave**@shawnmusgrave
03/05/2014

Few notice the "spotter car" from Manny Sousa's repo company as it scours Massachusetts parking lots, looking for vehicles whose owners have defaulted on their loans. Sousa's unmarked car is part of a technological revolution that goes well beyond the repossession business, transforming any industry that wants to check on the whereabouts of ordinary people. **READ MORE**

SILENCE IS GOLDEN

White House in no mood to debate big data and privacy at MIT



 **Cal Borchers** @CallumBorchers
03/04/2014



The White House says it wants a spirited debate about the benefits and risks of large-scale data collection. But the government officials who showed up at MIT Monday to kick off a 90-day federal review of big data and privacy displayed little appetite for substantive conversation. **READ**

MORE

Cambridge +5 More

to MIT to talk about privacy in age of Big Data



Michael Farrell @GlobeMBFarrell
03/03/2014



MIT is hosting a [workshop](#) today along with the White House to talk about privacy in the era of big data.

If you can't make the daylong event but want to hear what academics, privacy experts, and government officials have to say about keeping personal information safe in light of the National Security Agency surveillance revelations, [the event is streaming live here](#).

Don't expect panelists to dig too deeply into the legal issues around NSA activities. The agenda skews more technical. This afternoon

roundtable will discuss privacy enhancing
technology and how to protect privacy in the cloud.

But at 3:30 p.m. today, a panel will talk about

large scale analytics (the kind of thing the NSA does) that is scheduled to include John DeLong, director of compliance for the NSA, along with Chris Calabrese, legislative counsel with the American Civil Liberties Union. That has the makings of a good debate.

MIT



+3 More



MY BETA

UPWARD MOMENTUM

LevelUp gets new HQ in Financial District, shares growth stats



Kyle Alspach @kylealspach
16 MINUTES AGO



Mobile payments tech company [LevelUp](#) has

moved its headquarters to a new a location in
Boston's South End district



READ MORE

Startups

+

+6 More

BetaBoston

A BOSTON GLOBE SITE

The Boston Globe

Boston.com

BDCWire

RadioBDC

Contact Us

Advertise here

Privacy Policy

Ad Choices

Terms of Use

© 2014 Boston Globe Media Partners, LLC