ELECTRONIC FRONTIER FOUNDATION
DEFENDING YOUR RIGHTS IN THE DIGITAL WORLD (/)

OCTOBER 1, 2014 | BY DAVE MAASS (/ABOUT/STAFF/DAVE-MAASS)

ComputerCOP: The Dubious 'Internet Safety Software' That Hundreds of Police Agencies Have Distributed to Families

For years, local law enforcement agencies around the country have told parents that installing ComputerCOP (http://computercop.com/) software is the "first step" in protecting their children online.

Maricopa County Attorney's Office
Bill Montgomery, County Attorney
COMPUTER COP
Maricopa County Attorney's Office

ComputerCOP in Maricopa County, Arizona

Police chiefs, sheriffs, and district attorneys have handed out hundreds of thousands of copies of the disc to families for free at schools, libraries, and community events, usually as a part of an "Internet Safety" outreach initiative. The packaging typically features the agency's official seal and the chief's portrait, with a signed message warning of the "dark and dangerous off-ramps" of the Internet.

As official as it looks, ComputerCOP is actually just spyware, generally bought in bulk from a New York company that appears to do nothing but market this software to local government agencies.

The way ComputerCOP works is neither safe nor secure. It isn't particularly effective either, except for generating positive PR for the law enforcement agencies distributing it. As security software goes, we observed a product with a keystroke-capturing function, also called a "keylogger," that could place a family's personal information at extreme risk by transmitting what a user types over the Internet to third-party servers *without encryption*. That means many versions of ComputerCOP leave children (and their parents, guests, friends, and anyone using the affected computer) exposed to the same predators, identity thieves, and bullies that police claim the software protects against.

Furthermore, by providing a free keylogging program—especially one that operates without even the most basic security safeguards—law enforcement agencies are passing around what amounts to a spying tool that could easily be abused by people who want to snoop on spouses, roommates, or co-workers.

EFF conducted a security review of ComputerCOP while also following the paper trail of public records to see how widely the software has spread. Based on ComputerCOP's own marketing information, we identified approximately 245 agencies in more than 35 states, plus the U.S. Marshals, that have used public funds (often the proceeds from property seized during criminal investigations) to purchase and distribute ComputerCOP. One sheriff's department even bought a copy for every family in its county.

In investigating ComputerCOP, we also discovered misleading marketing material, including a letter of endorsement purportedly from the U.S. Department of Treasury, which has now issued a fraud alert over the document. ComputerCOP further claims an apparently nonexistent endorsement by the American Civil Liberties Union and an expired endorsement from the National Center for Missing and Exploited Children.

Law enforcement agencies have purchased a poor product, slapped their trusted emblems on it, and passed it on to everyday people. It's time for those law enforcement agencies to take away ComputerCOP's badge.

Donate to EFF
(https://supporters.eff.org/do

Stay in Touch

Email Address

Postal Code (optional)

SIGN UP NOW

NSA Spying

eff.org/nsa-spying
(/nsa-spying)

EFF is leading the fight against the NSA's illegal mass surveillance program. Learn more (/nsa-spying) about what the program is, how it works, and what you can do.

Follow EFF

In Melbourne on October 17? Join Australia's privacy activists to plot against data retention: https://privacy.electronworksh
(https://privacy.electronworks

OCT 6 @ 7:40PM

Are you Australian, or have any Australian friends? Here's how you can #StopDataRetention and #StopTheSpies: https://eff.org/r.sezp (https://eff.org/r.sezp)

OCT 6 @ 5:32PM

CloudFlare took a big step last week to make the web safer and more private, with free HTTPS for all its users. https://eff.org/r.e2sw (https://eff.org/r.e2sw)

OCT 6 @ 3:12PM

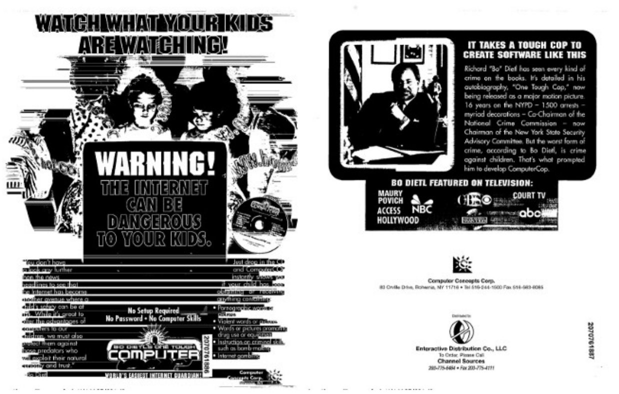
Twitter (https://twitter.com/eff)
Facebook (https://www.facebook.com/eff)
Identi.ca (https://identi.ca/eff)

Projects

Click here for a list of agencies that have distributed ComputerCOP. (https://www.eff.org/pages/whos-giving-out-computercop)

Click here for a guide to removing ComputerCOP from your computer. (https://www.eff.org/deeplinks/2014/09/computercop-howto)

What is ComputerCOP?



WATCH WHAT YOUR KIDS ARE WATCHING!

WARNING! THE INTERNET CAN BE DANGEROUS TO YOUR KIDS.

No Setup Required
No Password • No Computer Skills

BO DIETL'S ONE TOUGH COMPUTER

WORLD'S EASIEST INTERNET GUARDIAN!

- Pornographic words or
- Violent words or
- Words or pictures promoting drug use or
- Instruction on criminal skills such as bomb making
- Internet gambling

IT TAKES A TOUGH COP TO CREATE SOFTWARE LIKE THIS

Richard "Bo" Dietl has seen every kind of crime on the books. It's detailed in his autobiography, "One Tough Cop," now being released as a major motion picture. 16 years on the NYPD – 1500 arrests – myriad decorations – Co-Chairman of the National Crime Commission – now Chairman of the New York State Security Advisory Committee. But the worst form of crime, according to Bo Dietl, is crime against children. That's what prompted him to develop ComputerCop.

BO DIETL FEATURED ON TELEVISION:

MAURY POVICH
ACCESS HOLLYWOOD
NBC
COURT TV
abc

Computer Concepts Corp.

Enteractive Distribution Co., LLC
To Order, Please Call
Channel Sources

2070761886

2070761887

(http://legacy.library.ucsf.edu/tid/ohk67d00/pdf)Bo Dietl's One Tough Computer Cop (Source: UCSF Library (http://legacy.library.ucsf.edu/tid/ohk67d00/pdf))

(http://legacy.library.ucsf.edu/tid/ohk67d00/pdf)In an era when hackers use botnets, zero day exploits, and sophisticated phishing to compromise billions of online accounts, ComputerCOP is a software relic that not only offers little protection, but may actually expose your child's (and potentially your) most sensitive information to danger.

ComputerCOP's interface is a throwback to an earlier, clunkier age of computing. Indeed, its origins trace back 15 years, when software companies began to target a new demographic: parents worried about their children's exposure to all manner of danger and inappropriate material on the Internet.

When ComputerCOP debuted in the late 1990s, its original title was "Bo Dietl's One Tough ComputerCOP," which capitalized on the fame of celebrity New York detective, Bo Dietl, who had just had his career adapted into a major motion picture, "One Tough Cop," starring Stephen Baldwin. At the time, the program could only perform basic forensic searches of hard drives, but in the early 2000s, Bo Dietl's toughness was dropped from the title and a keylogger was added to the "deluxe" version of the package.

EFF obtained copies of ComputerCOP and related materials from law enforcement agencies on the East Coast, West Coast, and in Texas. Each one was branded to the specific department, but the software package was otherwise the same, containing two main elements:

Bloggers' Rights (/bloggers)

Coders' Rights (/issues/coders)

Follow EFF (/social-networks)

Free Speech Weak Links (/free-speech-weak-link)

Global Chokepoints (https://globalchokepoints.org/)

HTTPS Everywhere (/https-everywhere)

Medical Privacy Project (https://www.eff.org/issues/medical-privacy)

Open Wireless Movement (https://openwireless.org)

Patent Busting (https://w2.eff.org/patent/)

Student Activism (https://www.eff.org/fight)

Surveillance Self-Defense (https://ssd.eff.org)

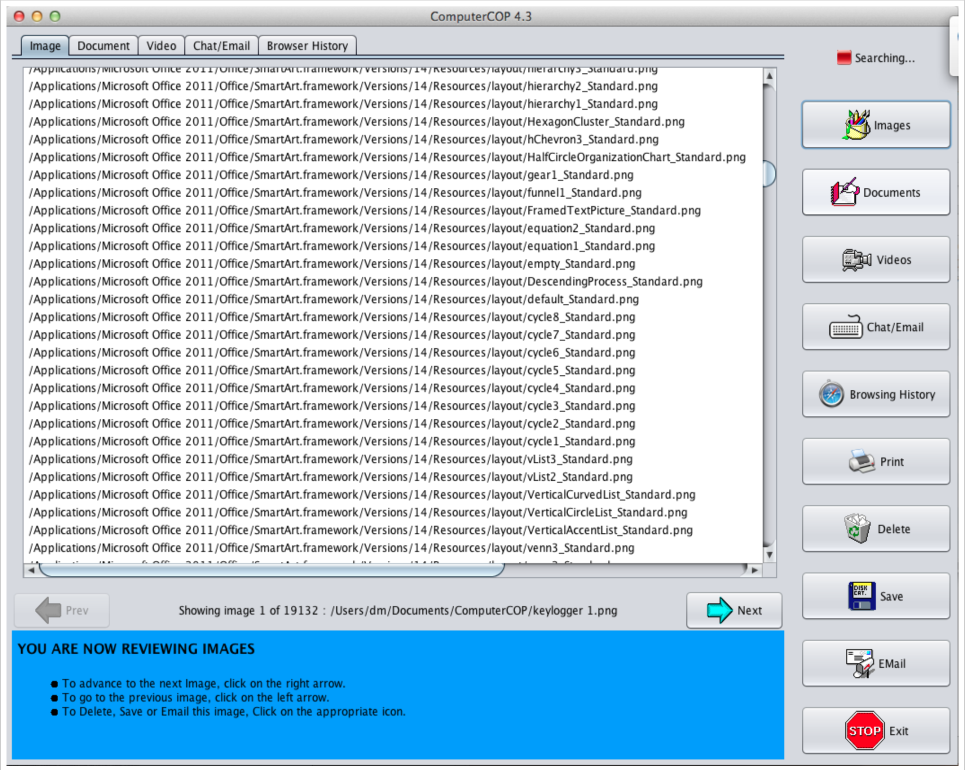
Takedown Hall of Shame (/takedowns)

Teaching Copyright (http://www.teachingcopyright.org/)

Transparency Project (https://www.eff.org/issues/transparency

Trolling Effects (https://trollingeffects.org)

Ways To Help (/helpout)



```
/Applications/Microsoft Office 2011/Office/SmartArt.framework/Versions/14/Resources/layout/hierarchy3_Standard.png
/Applications/Microsoft Office 2011/Office/SmartArt.framework/Versions/14/Resources/layout/hierarchy2_Standard.png
/Applications/Microsoft Office 2011/Office/SmartArt.framework/Versions/14/Resources/layout/hierarchy1_Standard.png
/Applications/Microsoft Office 2011/Office/SmartArt.framework/Versions/14/Resources/layout/HexagonCluster_Standard.png
/Applications/Microsoft Office 2011/Office/SmartArt.framework/Versions/14/Resources/layout/hChevron3_Standard.png
/Applications/Microsoft Office 2011/Office/SmartArt.framework/Versions/14/Resources/layout/HalfCircleOrganizationChart_Standard.png
/Applications/Microsoft Office 2011/Office/SmartArt.framework/Versions/14/Resources/layout/gear1_Standard.png
/Applications/Microsoft Office 2011/Office/SmartArt.framework/Versions/14/Resources/layout/funnel1_Standard.png
/Applications/Microsoft Office 2011/Office/SmartArt.framework/Versions/14/Resources/layout/FramedTextPicture_Standard.png
/Applications/Microsoft Office 2011/Office/SmartArt.framework/Versions/14/Resources/layout/equation2_Standard.png
/Applications/Microsoft Office 2011/Office/SmartArt.framework/Versions/14/Resources/layout/equation1_Standard.png
/Applications/Microsoft Office 2011/Office/SmartArt.framework/Versions/14/Resources/layout/empty_Standard.png
/Applications/Microsoft Office 2011/Office/SmartArt.framework/Versions/14/Resources/layout/DescendingProcess_Standard.png
/Applications/Microsoft Office 2011/Office/SmartArt.framework/Versions/14/Resources/layout/default_Standard.png
/Applications/Microsoft Office 2011/Office/SmartArt.framework/Versions/14/Resources/layout/cycle8_Standard.png
/Applications/Microsoft Office 2011/Office/SmartArt.framework/Versions/14/Resources/layout/cycle7_Standard.png
/Applications/Microsoft Office 2011/Office/SmartArt.framework/Versions/14/Resources/layout/cycle6_Standard.png
/Applications/Microsoft Office 2011/Office/SmartArt.framework/Versions/14/Resources/layout/cycle5_Standard.png
/Applications/Microsoft Office 2011/Office/SmartArt.framework/Versions/14/Resources/layout/cycle4_Standard.png
/Applications/Microsoft Office 2011/Office/SmartArt.framework/Versions/14/Resources/layout/cycle3_Standard.png
/Applications/Microsoft Office 2011/Office/SmartArt.framework/Versions/14/Resources/layout/cycle2_Standard.png
/Applications/Microsoft Office 2011/Office/SmartArt.framework/Versions/14/Resources/layout/cycle1_Standard.png
/Applications/Microsoft Office 2011/Office/SmartArt.framework/Versions/14/Resources/layout/vList3_Standard.png
/Applications/Microsoft Office 2011/Office/SmartArt.framework/Versions/14/Resources/layout/vList2_Standard.png
/Applications/Microsoft Office 2011/Office/SmartArt.framework/Versions/14/Resources/layout/VerticalCurvedList_Standard.png
/Applications/Microsoft Office 2011/Office/SmartArt.framework/Versions/14/Resources/layout/VerticalCircleList_Standard.png
/Applications/Microsoft Office 2011/Office/SmartArt.framework/Versions/14/Resources/layout/VerticalAccentList_Standard.png
/Applications/Microsoft Office 2011/Office/SmartArt.framework/Versions/14/Resources/layout/venn3_Standard.png
```

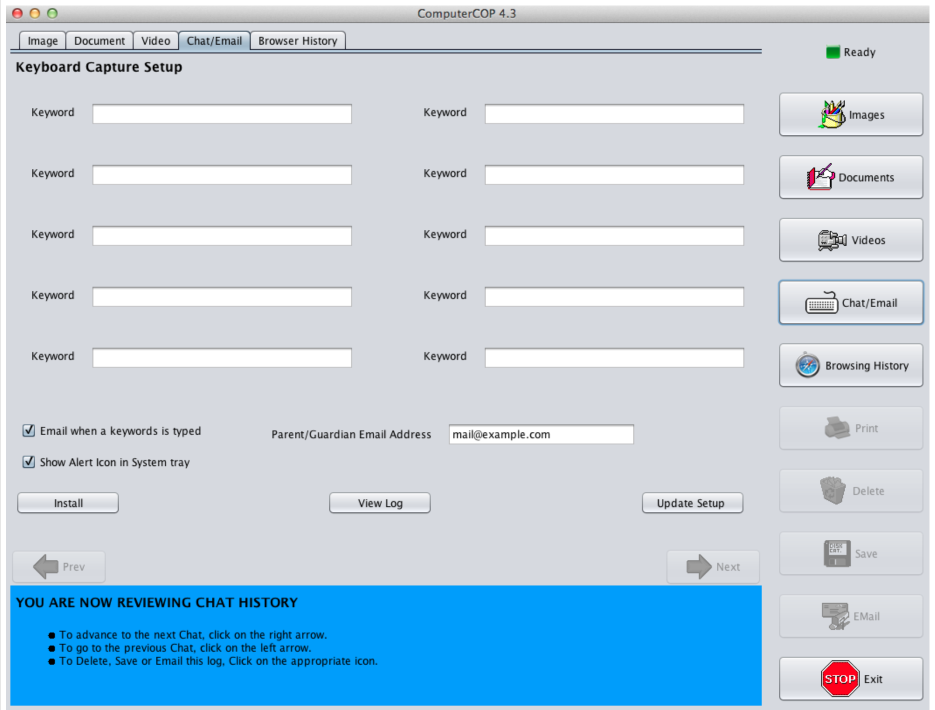
Showing image 1 of 19132 : /Users/dm/Documents/ComputerCOP/keylogger 1.png

YOU ARE NOW REVIEWING IMAGES

- To advance to the next Image, click on the right arrow.
- To go to the previous image, click on the left arrow.
- To Delete, Save or Email this image, Click on the appropriate icon.

ComputerCOP's image search (OS version) turned up a haystack of 19,000 files

"Basic" Search Functions: ComputerCOP's search utility does not require installation and can run right off the CD-ROM. The tool allows the user to review recent images and videos downloaded to the computer, but it will also scan the hard drive looking for documents containing phrases in ComputerCOP's dictionary of thousand of keywords related to drugs, sex, gangs, and hate groups. While that feature may sound impressive, in practice the software is unreliable. On some computer systems, it produces a giant haystack of false positives, including flagging items as innocuous as raw computer code. On other systems, it will only produce a handful of results while typing keywords such as "drugs" into Finder or File Explorer will turn up a far larger number of hits. While the marketing materials claim that this software will allow you to view what web pages your child visits, that's only true if the child is using Internet Explorer or Safari. The image search will potentially turn up tens of thousands of hits because it can't distinguish between images children have downloaded and the huge collection of icons and images that are typically part of the software on your computer.



Keyboard Capture Setup

☑ Email when a keywords is typed

Parent/Guardian Email Address mail@example.com

☑ Show Alert Icon in System tray

YOU ARE NOW REVIEWING CHAT HISTORY

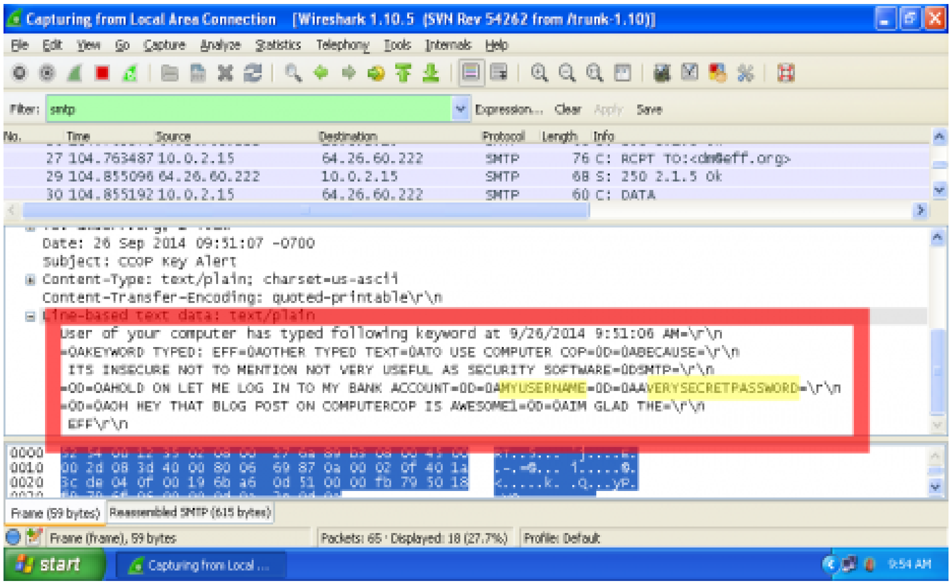
- To advance to the next Chat, click on the right arrow.
- To go to the previous Chat, click on the left arrow.
- To Delete, Save or Email this log, Click on the appropriate icon.

Interface for installing ComputerCOP keylogger

KeyAlert: ComputerCOP's KeyAlert keylogging program does require installation and, if the user isn't careful, it will collect keystrokes from all users of the computer, not just children. When running on a Windows machine, the software stores full key logs (https://www.eff.org/files/2014/09/26/sample_key_log.png) unencrypted on the user's hard drive. When running on a Mac, the software encrypts these key logs on the user's hard drive, but these can be decrypted with the underlying software's default password. On both Windows and Mac computers, parents can also set ComputerCOP up to email them whenever chosen keywords are typed. When that happens, the software transmits the key logs, unencrypted, to a third-party server, which then sends the email. KeyAlert is in included in the "deluxe," "premium," and "presentation" versions of the software.

The keylogger is problematic on multiple levels. In general, keyloggers are commonly a tool of spies, malicious hackers, and (occasionally) nosy employers. ComputerCOP does not have the ability to distinguish between children and adults, so law enforcement agencies that distribute the software are also giving recipients the tools to spy on other adults who use a shared computer, such as spouses, roommates, and coworkers. ComputerCOP addresses this issue with a pop-up warning that using it on non-consenting adults could run afoul of criminal laws, but that's about it.

The lack of encryption is even more troubling. Security experts universally agree that a user should never store passwords and banking details or other sensitive details unprotected on one's hard drive, but that's exactly what ComputerCOP does by placing everything someone types in a folder. The email alert system further weakens protections by logging into a third-party commercial server. When a child with ComputerCOP installed on their laptop connects to public Wi-Fi, any sexual predator, identity thief, or bully with freely available packet-sniffing software can grab those key logs right out of the air.



```
No.  Time        Source        Destination    Protocol  Length  Info
  27 104.763487 10.0.2.15     64.26.60.222   SMTP          76 C: RCPT TO:<dm@eff.org>
  29 104.855096 64.26.60.222  10.0.2.15      SMTP          68 S: 250 2.1.5 Ok
  30 104.855192 10.0.2.15     64.26.60.222   SMTP          60 C: DATA
```

```
   Date: 26 Sep 2014 09:51:07 -0700
   Subject: CCOP Key Alert
⊞  Content-Type: text/plain; charset=us-ascii
   Content-Transfer-Encoding: quoted-printable\r\n
⊟  Line-based text data: text/plain
     User of your computer has typed following keyword at 9/26/2014 9:51:06 AM=\r\n
     =0AKEYWORD TYPED: EFF=0AOTHER TYPED TEXT=0ATO USE COMPUTER COP=0D=0ABECAUSE=\r\n
      ITS INSECURE NOT TO MENTION NOT VERY USEFUL AS SECURITY SOFTWARE=0DSMTP=\r\n
     =0D=0AHOLD ON LET ME LOG IN TO MY BANK ACCOUNT=0D=0AMYUSERNAME=0D=0AAVERYSECRETPASSWORD=\r\n
     =0D=0AOH HEY THAT BLOG POST ON COMPUTERCOP IS AWESOME1=0D=0AIM GLAD THE=\r\n
      EFF\r\n
```

```
0000
0010  00 2d 08 3d 40 00 80 06  69 87 0a 00 02 0f 40 1a   .-.=@... i.....@.
0020  3c da 04 0f 00 19 6b a6  0d 51 00 00 fb 79 50 18   <.....k. .Q...yP.
```

Example of intercepted, unencrypted keylogs using Wireshark, a free packet sniffer

The software does not appear in any of the major malware/spyware databases we tested, so it can't be detected with a normal virus scan.

Eight months ago, we contacted Stephen DelGiorno, the head of ComputerCOP operations, and informed him of these problems. He denied there was an issue.

"ComputerCOP software doesn't give sexual predator [sic] or identity thieves more access to children's computers, as our .key logger [sic] works with the existing email and Internet access services that computer user has already engaged," he wrote via email.

He further said that ComputerCOP would update the software's licensing agreement to say "that no personal information is obtained nor stored by ComputerCOP."

These are unacceptable, and fairly nonsensical, answers from a company that claims to be a leader in child safety software. Even if the company isn't storing data, as it claims, information captured by the keylogger still passes through a commercial server when the target types a keyword. Further, the keylogger actually may undermine other services' security measures.

Some of the most common online services, such as Facebook, Twitter, and Gmail (as well as most financial sites), use HTTPS by default, automatically encrypting communications between users and those websites. In fact, one of the truly effective tools parents can use to protect their children is HTTPS Everywhere (https://www.eff.org/https-everywhere), an EFF plug-in that makes an Internet browser connect by default to secure versions of websites.

But HTTPS is rendered ineffective with ComputerCOP, because ComputerCOP captures text as it is being typed, *before* it has been encrypted. While HTTPS is protecting the users' connection to a website, ComputerCOP separately transmits that same communication unprotected whenever a keyword is triggered.

In EFF's testing, we were able to snatch passwords (faked ones, of course) with shocking ease.

Law Enforcement and ComputerCOP

CHAT ROOMS EMAIL YOUTUBE MYSPACE FACEBOOK
COMPUTER COP
FACEBOOK INSTANT MESSENGER CHAT ROOMS EMAIL

Privacy info. (https://www.eff.org/deeplinks/2008/02/embedded-video-and-your-privacy) This embed will serve content from *youtube-nocookie.com (http://www.youtube-nocookie.com/embed/TUZIooo9jgM?rel=0)*

A compilation of ComputerCOP promotional videos

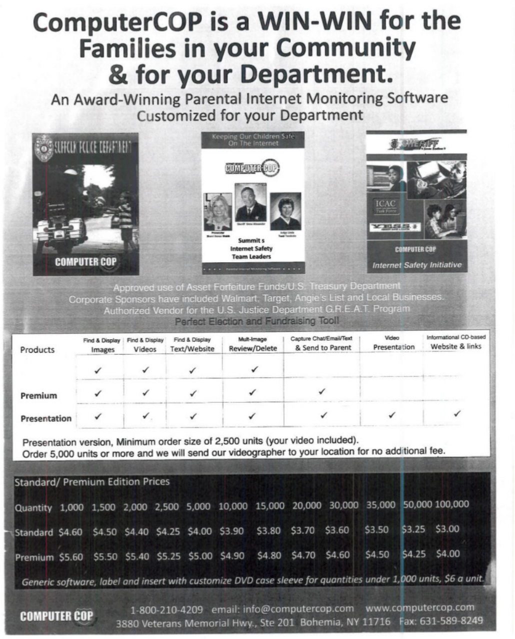
"The ComputerCOP outreach program is the best way for Parents/Guardians to monitor their children's activity online and bring positive media attention to your Office," DelGiorno writes in the first line of the form letter his company sends to law enforcement agencies.

ComputerCOP's business model works like this: the company contracts with police and district attorneys around the country, particularly ones that have federal grants or special funds to spend, such as asset forfeiture windfalls (police often describe this as money seized from drug dealers). Agencies then buy the software in bulk, usually between 1,000 and 5,000 at a time, and give it out for free in their communities. Agencies often tell the press that the software has a value of $40, even though they pay only a few bucks per copy and the software is not available through any major online store other than eBay (where surplus new copies are going for as little as $.99) (https://www.eff.org/files/2014/09/29/computer_cop_deluxe_internet_security_parental_internet_monitoring_software_ebay_0.pdf). Even ComputerCOP's online store (https://www.eff.org/files/2014/09/29/ccop-contentshelf.com_.pdf) is currently broken.

There is no official central repository for data about which agencies have purchased the software, how many copies they've distributed, or how much they have spent. Based on ComputerCOP's own online map of agencies, as well as online searches and public records requests, we have identified approximately 245 agencies in more than 35 states that purchased ComputerCOP. (After we began our investigation, ComputerCOP took the map (https://web.archive.org/web/20130906170047/http://computercop.com/maps.html) offline, promising an updated one soon.)

In February, DelGiorno told EFF the keystroke-logging feature was a recent addition to the software and that most of the units he's sold did not include the feature. That doesn't seem to jibe with ComputerCOP's online footprint. Archive.org's WayBack Machine (https://web.archive.org/web/20010124045000/http://www.computercop.com/productdeluxe.html) shows that keystroke capture was advertised on ComputerCOP.com as far back as 2001. Although some versions of ComputerCOP do not have the keylogger function, scores of press releases and regional news articles from across the country discuss the software's ability to capture a child's conversations.

Among the most notable in the last two years: the Maricopa County Attorney's Office (http://www.maricopacountyattorney.org/newsroom/newsletters/2013/2013-09-newsletter.html#topic4) in Arizona, the San Diego District Attorney's Office (http://www.sdcda.org/preventing/internet-safety.html) in California, the Jackson County Sheriff's Office (http://www.kshb.com/news/education/computer-software-helps-protect-children-from-online-predators) in Missouri and the Bexar County District Attorney’s Office (http://home.bexar.org/da/release_2012-12-19_InternetSafety.html) in Texas each purchased 5,000 copies at a cost of $25,000 per agency. Bexar County even has an interactive map (http://home.bexar.org/da/computer_cop.html) on its website showing the dozens of locations where ComputerCOP can be picked up for free.


SUFFOLK POLICE DEPARTMENT
COMPUTER COP
Keeping Our Children Safe On The Internet
COMPUTER COP
Summit s
Internet Safety
Team Leaders
ICAC
Task Force
COMPUTER COP
Internet Safety Initiative

ComputerCOP is a WIN-WIN for the Families in your Community & for your Department.

An Award-Winning Parental Internet Monitoring Software
Customized for your Department

Approved use of Asset Forfeiture Funds/U.S. Treasury Department
Corporate Sponsors have included Walmart, Target, Angie's List and Local Businesses.
Authorized Vendor for the U.S. Justice Department G.R.E.A.T. Program
Perfect Election and Fundraising Tool!

Products	Find & Display Images	Find & Display Videos	Find & Display Text/Website	Mult-Image Review/Delete	Capture Chat/Email/Text & Send to Parent	Video Presentation	Informational CD-based Website & links
	✓	✓	✓	✓			
Premium	✓	✓	✓	✓	✓		
Presentation	✓	✓	✓	✓	✓	✓	✓

Presentation version, Minimum order size of 2,500 units (your video included).
Order 5,000 units or more and we will send our videographer to your location for no additional fee.

Standard/ Premium Edition Prices

Quantity	1,000	1,500	2,000	2,500	5,000	10,000	15,000	20,000	30,000	35,000	50,000	100,000
Standard	$4.60	$4.50	$4.40	$4.25	$4.00	$3.90	$3.80	$3.70	$3.60	$3.50	$3.25	$3.00
Premium	$5.60	$5.50	$5.40	$5.25	$5.00	$4.90	$4.80	$4.70	$4.60	$4.50	$4.25	$4.00

Generic software, label and insert with customize DVD case sleeve for quantities under 1,000 units, $6 a unit.

COMPUTER COP
1-800-210-4209 email: info@computercop.com www.computercop.com
3880 Veterans Memorial Hwy., Ste 201 Bohemia, NY 11716 Fax: 631-589-8249

(https://www.eff.org/files/2014/09/26/computercop_promo_poster.jpg)ComputerCOP promotional poster

Other agencies have purchased the software in even larger quantities. In 2008, the Highlands County Sheriff in Florida spent $42,000 to purchase 10,000 copies, or, as one newspaper put it, “enough computer disks for every parent of every school child in Highlands County.” The Alaska Department of Public Safety bought enough copies for it to be available at every "school, public library and police agency" in the state.

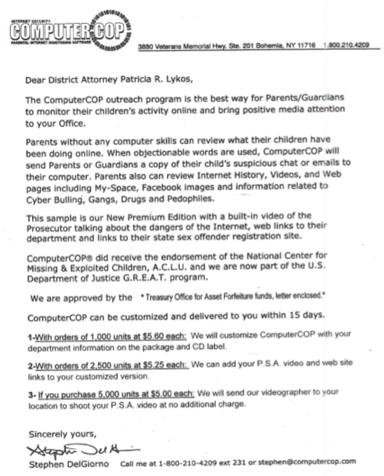
Since 2007, Suffolk County Sheriff Vincent DeMarco’s office in New York, where ComputerCOP is based, has bought 43,000 copies of the software (http://www.suffolkcountyny.gov/sheriff/PressReleases/tabid/909/ctl/details/itemid/130/mid/1989/sheriff-demarco-kicks-off-internet-safety-initiative.aspx)—a fact trumpeted in DeMarco’s reelection campaign materials (https://web.archive.org/web/20140924204603/http://sheriffvincentdemarco.com/about.htm). ComputerCOP’s parent company directly donated to DeMarco’s campaign at least (https://www.eff.org/files/2014/09/05/demarco1.png) nine (https://www.eff.org/files/2014/09/05/demarco2.png) times (https://www.eff.org/files/2014/09/05/demarco3.png) over the same period.

Indeed, ComputerCOP markets itself as the “perfect election and fundraising tool.” As part of the package, when a law enforcement agency buys a certain amount of copies, ComputerCOP will send out a camera crew to record an introduction video with the head of the department. The discs are also customized to prominently feature the head of the agency, who can count on a solid round of local press coverage about the giveaway.

Delgiorno also said he would contact his accountant to get a list of which agencies purchased which version of ComputerCOP (i.e. the versions with the keylogger versus those without). Eight months later, we're still waiting.

Dubious Claims

Through a public records act request, EFF obtained a copy of the marketing materials



3880 Veterans Memorial Hwy. Ste. 201 Bohemia, NY 11716 1.800.210.4209

Dear District Attorney Patricia R. Lykos,

The ComputerCOP outreach program is the best way for Parents/Guardians to monitor their children's activity online and bring positive media attention to your Office.

Parents without any computer skills can review what their children have been doing online. When objectionable words are used, ComputerCOP will send Parents or Guardians a copy of their child's suspicious chat or emails to their computer. Parents also can review Internet History, Videos, and Web pages including My-Space, Facebook images and information related to Cyber Bulling, Gangs, Drugs and Pedophiles.

This sample is our New Premium Edition with a built-in video of the Prosecutor talking about the dangers of the Internet, web links to their department and links to their state sex offender registration site.

ComputerCOP® did receive the endorsement of the National Center for Missing & Exploited Children, A.C.L.U. and we are now part of the U.S. Department of Justice G.R.E.A.T. program.

We are approved by the * Treasury Office for Asset Forfeiture funds, letter enclosed.*

ComputerCOP can be customized and delivered to you within 15 days.

1-With orders of 1,000 units at $5.60 each: We will customize ComputerCOP with your department information on the package and CD label.

2-With orders of 2,500 units at $5.25 each: We can add your P.S.A. video and web site links to your customized version.

3- If you purchase 5,000 units at $5.00 each: We will send our videographer to your location to shoot your P.S.A. video at no additional charge.

Sincerely yours,

Stephen DelGiorno Call me at 1-800-210-4209 ext 231 or stephen@computercop.com

(https://www.eff.org/files/2014/09/24/computercop_lykos_letter.png)ComputerCOP letter, 2011

(https://www.eff.org/files/2014/09/30/harris_county_records.pdf) submitted by ComputerCOP to the Harris County District Attorney's office in Texas, which purchased 5,000 copies in 2011. The documents reveal several dubious and outdated claims.

For one, ComputerCOP claims that it is endorsed by the American Civil Liberties Union (ACLU) and that it is the only software product supported by the National Center for Missing and Exploited Children (NCMEC).

When asked about the origin of the ACLU endorsement, DelGiorno told EFF that someone from the ACLU recommended the software in a *Newsday* article as the "most non-intrusive of the products as it did not filter web pages nor block user access to them." EFF contacted *Newsday*, which was unable to locate any such article, as well several branches of the ACLU, all of which denied any such endorsement.

On the eve of publication of this report, DelGiorno told reporter Alice Brennan at *Fusion* (http://fusion.net/video/19094/who-needs-the-nsa-anyone-could-spy-on-your-kids-thanks-to-computercop/) that the endorsement came from Kary Moss, executive director of the ACLU of Michigan, citing a 2005 story (https://web.archive.org/web/20050204171049/http://www.freep.com/news/childrenfirst/cybercop21e_20041221.htm) in the *Detroit Free Press*. However, in the article, Moss is endorsing the idea that parents should take responsibility for monitoring their children as opposed to relying on the government to act as a babysitter.

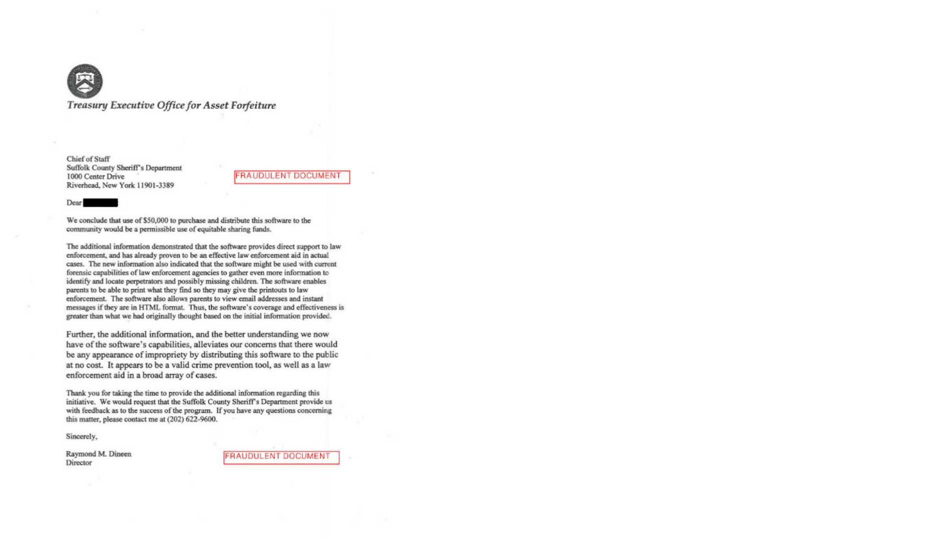
"I can say unequivocally that it was not an endorsement of the product," ACLU of Michigan Deputy Director Rana Elmir told EFF. "Our position as an organization is not to endorse technology like this."

NCMEC told EFF that in 1998 it did allow ComputerCOP to use its name for a one-year period, but has not had any contact with the company over the last 15 years. A NCMEC attorney said the organization was unaware that ComputerCOP was still advertising its imprimatur and that it would tell ComputerCOP to stop using it immediately.

In its promotional packet, ComputerCOP includes a letter from the Treasury Executive Office for Asset Forfeiture, in which the head of the division calls the software an "effective law enforcement aid" and a "valid crime prevention tool" that will "identify and locate perpetrators and possibly missing children." The uncharacteristically positive nature of the letter caused EFF to examine it closer and, as it turns out, the document had been significantly altered.

In an email exchange, DelGiorno acknowledged that ComputerCOP had taken a prior letter from the Treasury Department, highlighted text and "recreated the letterhead to make more it presentable for other agencies to view." In doing so, ComputerCOP removed the 2001 date stamp from the letter. As a result, law enforcement agencies were unaware that the letter was outdated by more than a decade and that the agency head who signed it had long left office.[1]

Through the Freedom of Information Act, EFF is seeking the unaltered letter, as well as any material ComputerCOP submitted to the Treasury Department. So far the agency has been unable to locate those file and ComputerCOP would not provide a copy of the original letter to



Treasury Executive Office for Asset Forfeiture

Chief of Staff
Suffolk County Sheriff's Department
1000 Center Drive
Riverhead, New York 11901-3389

FRAUDULENT DOCUMENT

Dear [redacted]

We conclude that use of $50,000 to purchase and distribute this software to the community would be a permissible use of equitable sharing funds.

The additional information demonstrated that the software provides direct support to law enforcement, and has already proven to be an effective law enforcement aid in actual cases. The new information also indicated that the software might be used with current forensic capabilities of law enforcement agencies to gather even more information to identify and locate perpetrators and possibly missing children. The software enables parents to be able to print what they find so they may give the printouts to law enforcement. The software also allows parents to view email addresses and instant messages if they are in HTML format. Thus, the software's coverage and effectiveness is greater than what we had originally thought based on the initial information provided.

Further, the additional information, and the better understanding we now have of the software's capabilities, alleviates our concerns that there would be any appearance of impropriety by distributing this software to the public at no cost. It appears to be a valid crime prevention tool, as well as a law enforcement aid in a broad array of cases.

Thank you for taking the time to provide the additional information regarding this initiative. We would request that the Suffolk County Sheriff's Department provide us with feedback as to the success of the program. If you have any questions concerning this matter, please contact me at (202) 622-9600.

Sincerely,

Raymond M. Dineen
Director

FRAUDULENT DOCUMENT

(https://www.eff.org/files/2014/09/24/fraudulent_teoaf_letter_redacted.jpg)Letter marked "fraudulent" by Treasury Dept.

EFF.

However, after we submitted the suspicious letter to the Treasury Department, the Treasury Department's Inspector General issued a fraud alert (http://www.treasury.gov/about/organizational-structure/ig/Pages/fraud-alerts_index2.aspx) over ComputerCOP, including a copy of the letter with the words "Fraudulent Document" stamped on it in red.

ComputerCOP Conclusions

We estimate somewhere between a few hundred thousand and more than a million copies of ComputerCOP have been purchased by law enforcement agencies across the United States, but it's difficult to say how many individual people have been exposed by the software's vulnerabilities.

In our tests, ComputerCOP was so unwieldy to use that it's possible that very few people actually use it. But even if it's a pointless giveaway from the police, it's still being purchased with our tax dollars and other public funds. As law enforcement agencies around the country face budgetary shortfalls, spending $25,000 on an ineffective product is not only unwise, but fiscally irresponsible.

Law enforcement agencies should cease distributing copies immediately and tell parents not to use it. Any local media outlet that reported on ComputerCOP should consider alerting parents to its dangers. The Treasury Department should reexamine its approval of ComputerCOP as a permissible use of funds from the federal equitable sharing program.

There are certainly risks for kids on the Internet, and indeed for adults too. Let's not make it easier for villains with bogus safeguards.

EFF Staff Technologist Jeremy Gillula and Web Developer Bill Budington conducted the security analysis of this software.

Clarification: In the third to last paragraph we added "and other public funds" to clarify that law enforcement agencies use a variety of funding sources to purchase the software, including seized assets, appropriations from governing bodies, federal grants and the rare private donation to an agency.

[1] In 2010, the Treasury Department did issue a new letter authorizing ComputerCOP as a permissible use of asset forfeiture money, but this time the department clearly stated that it does not endorse the product "in any way" and that law enforcement agencies should make sure that the software does not run afoul of local laws.

MORE DEEPLINKS POSTS LIKE THIS

OCTOBER 2014

How to Remove ComputerCOP (/deeplinks/2014/09/computercop-howto)

JUNE 2012

Can Apple Refuse to Sell a Laptop to an Iranian Citizen? Maybe. (/deeplinks/2012/06/can-apple-refuse-sell-laptop-iranian-citizen-maybe)

OCTOBER 2012

EFF and MuckRock Have Filed Over 200 Records Requests On Drones And The Results Are Pouring In (/deeplinks/2012/10/eff-and-muckrock-have-filed-over-200-public-records-requests-surveillance-drones)

FEBRUARY 2013

California Sheriff Faces Loud Privacy Protests Against Drone Plans (/deeplinks/2013/02/alameda-county-california-sheriff-drone-protests)

SEPTEMBER 2011

California Supreme Court Agrees to Hear Electronic Public Records Case (/deeplinks/2011/09/california-supreme-court-agrees-hear-computer)

RECENT DEEPLINKS POSTS

OCT 6, 2014

How CloudFlare Moved the Web Toward Ubiquitous HTTPS (/deeplinks/2014/10/how-cloudflare-moved-web-toward-ubiquitous-https)

OCT 6, 2014

Stop the Spies: Australians Rise Up Against Mandatory Data Retention (/deeplinks/2014/10/stop-spies-australians-rise-against-mandatory-data-retention)

OCT 3, 2014

EU-US Trade Negotiations Continue Shutting out the Public—When Will They Learn? (/deeplinks/2014/10/eu-us-trade-negotiations-continue-shutting-out-public-when-will-they-learn)

OCT 3, 2014

A Wikipedia Edit-a-thon for the Zone 9 Bloggers, A Great Way to Raise Awareness (/deeplinks/2014/10/wikipedia-edit-thon-zone-9-bloggers-great-way-raise-awareness)

OCT 2, 2014

Knowledge Should Not Be Trapped Behind A Paywall: Get Ready For Open Access Week (/deeplinks/2014/10/knowledge-should-not-be-trapped-behind-paywall-get-ready-open-access-week)

DEEPLINKS TOPICS

Abortion Reporting (/deeplinks/abortion-reporting)

Analog Hole (/deeplinks/analog-hole)

Anonymity (/deeplinks/anonymity)

Anti-Counterfeiting Trade Agreement (/deeplinks/anti-counterfeiting-trade-agreement)

Biometrics (/deeplinks/biometrics)

Bloggers' Rights (/deeplinks/bloggers%27-rights)

Broadcast Flag (/deeplinks/broadcast-flag)

Broadcasting Treaty (/deeplinks/broadcasting-treaty)

CALEA (/deeplinks/calea)

Cell Tracking (/deeplinks/cell-tracking)

Coders' Rights Project (/deeplinks/coders%27-rights-project)

Computer Fraud And Abuse Act Reform (/deeplinks/computer-fraud-and-abuse-act-reform)

Content Blocking (/deeplinks/content-blocking)

Copyright Trolls (/deeplinks/copyright-trolls)

FAQs for Lodsys Targets (/deeplinks/faqs-for-lodsys-targets)

File Sharing (/deeplinks/file-sharing)

Fixing Copyright? The 2013-2014 Copyright Review Process (/deeplinks/fixing-copyright?-the-2013-2014-copyright-review-process=)

Free Speech (/deeplinks/free-speech)

FTAA (/deeplinks/ftaa)

Genetic Information Privacy (/deeplinks/genetic-information-privacy)

Hollywood v. DVD (/deeplinks/hollywood-v.-dvd)

How Patents Hinder Innovation (Graphic) (/deeplinks/how-patents-hinder-innovation-%28graphic%29)

Innovation (/deeplinks/innovation)

International (/deeplinks/international)

International Privacy Standards (/deeplinks/international-privacy-standards)

Internet Governance Forum (/deeplinks/internet-governance-forum)

Law Enforcement Access (/deeplinks/law-enforcement-access)

Pen Trap (/deeplinks/pen-trap)

Policy Analysis (/deeplinks/policy-analysis)

Printers (/deeplinks/printers)

Privacy (/deeplinks/privacy)

Public Health Reporting and Hospital Discharge Data (/deeplinks/public-health-reporting-and-hospital-discharge-data)

Reading Accessibility (/deeplinks/reading-accessibility)

Real ID (/deeplinks/real-id)

RFID (/deeplinks/rfid)

Search Engines (/deeplinks/search-engines)

Search Incident to Arrest (/deeplinks/search-incident-to-arrest)

Section 230 of the Communications Decency Act (/deeplinks/section-230-of-the-communications-decency-act)

Security (/deeplinks/security)

Social Networks (/deeplinks/social-networks)

SOPA/PIPA: Internet Blacklist Legislation (/deeplinks/sopa/pipa%3A-internet-blacklist-legislation)

State-Sponsored Malware (/deeplinks/state-sponsored-

Council of Europe (/deeplinks/council-of-europe)

Cyber Security Legislation (/deeplinks/cyber-security-legislation)

CyberSLAPP (/deeplinks/cyberslapp)

Defend Your Right to Repair! (/deeplinks/defend-your-right-to-repair%21)

Defending Digital Voices (/deeplinks/defending-digital-voices)

Development Agenda (/deeplinks/development-agenda)

Digital Books (/deeplinks/digital-books)

Digital Radio (/deeplinks/digital-radio)

Digital Video (/deeplinks/digital-video)

DMCA (/deeplinks/dmca)

DMCA Rulemaking (/deeplinks/dmca-rulemaking)

Do Not Track (/deeplinks/do-not-track)

DRM (/deeplinks/drm)

E-Voting Rights (/deeplinks/e-voting-rights)

EFF Europe (/deeplinks/eff-europe)

Encrypting the Web (/deeplinks/encrypting-the-web)

Export Controls (/deeplinks/export-controls)

Fair Use and Intellectual Property: Defending the Balance (/deeplinks/fair-use-and-intellectual-property%3A-defending-the-balance)

Legislative Solutions for Patent Reform (/deeplinks/legislative-solutions-for-patent-reform)

Locational Privacy (/deeplinks/locational-privacy)

Mandatory Data Retention (/deeplinks/mandatory-data-retention)

Mandatory National IDs and Biometric Databases (/deeplinks/mandatory-national-ids-and-biometric-databases)

Mass Surveillance Technologies (/deeplinks/mass-surveillance-technologies)

Medical Privacy (/deeplinks/medical-privacy)

National Security and Medical Information (/deeplinks/national-security-and-medical-information)

National Security Letters (/deeplinks/national-security-letters)

Net Neutrality (/deeplinks/net-neutrality)

No Downtime for Free Speech (/deeplinks/no-downtime-for-free-speech)

NSA Spying (/deeplinks/nsa-spying)

OECD (/deeplinks/oecd)

Online Behavioral Tracking (/deeplinks/online-behavioral-tracking)

Open Access (/deeplinks/open-access)

Open Wireless (/deeplinks/open-wireless)

Patent Busting Project (/deeplinks/patent-busting-project)

Patent Trolls (/deeplinks/patent-trolls)

Patents (/deeplinks/patents)

PATRIOT Act (/deeplinks/patriot-act)

malware)

Student and Community Organizing (/deeplinks/student-and-community-organizing)

Surveillance and Human Rights (/deeplinks/surveillance-and-human-rights)

Surveillance Drones (/deeplinks/surveillance-drones)

Terms Of (Ab)Use (/deeplinks/terms-of-%28ab%29use)

Test Your ISP (/deeplinks/test-your-isp)

The "Six Strikes" Copyright Surveillance Machine (/deeplinks/the-%22six-strikes%22-copyright-surveillance-machine)

The Global Network Initiative (/deeplinks/the-global-network-initiative)

The Law and Medical Privacy (/deeplinks/the-law-and-medical-privacy)

Trans-Pacific Partnership Agreement (/deeplinks/trans-pacific-partnership-agreement)

Transparency (/deeplinks/transparency)

Travel Screening (/deeplinks/travel-screening)

Trusted Computing (/deeplinks/trusted-computing)

Uncategorized (/deeplinks/uncategorized)

Video Games (/deeplinks/video-games)

Wikileaks (/deeplinks/wikileaks)

WIPO (/deeplinks/wipo)