THE PRIVACY RIGHTS INVESTIGATION

Sun, 01 Dec 2013 16:00:00, newstips66, [category: afghanistan, category: brotopia, category: elon-musk, category: energy-dept-slush-fund, category: google-alphabet, category: hired-assassins, category: idea-theft, category: lithium-batteries, category: political-bribes, category: sony_pictures, category: stanford_univ_bribes, category: web-spying, category: worldnews]

Your Daily Privacy Theft! Who Hacks You? "Data-Rape": Bulk harvesting your personal data property!

----

60 Minutes blows "data-rape" & "privacy-rape" wide open! The Data brokers: Easily stealing & selling your sexual, mental, medical and life data every day. See the video below:

http://www.youtube.com/watch?v=qe_iLgpnjBI

See the entire 60 Minutes story here:

http://www.cbsnews.com/videos/the-data-brokers-selling-your-personal-information

http://www.youtube.com/watch?v=_YffwdsnKXo

SEE ALSO: WHY YOU MUST CARE, HOW IT PERSONALLY AFFECTS YOU >>>

SEE ALSO: HOW TECH COMPANIES BRAINWASH YOU >>>

LINK TO THIS PAGE: http://wp.me/P4e1uX-xl

Class Action Lawsuits in preparation, and now being filed, against Dot.Com companies that bulk harvest your personal "private data property" without paying you.

You own your personal marketing data like you own your house. Companies can't rent your house without your permission. It is not legal for them to *"look like"* they are asking for your permission, if they do so in a manner meant to confuse you.

You own your personal private use data like you own your own hair. Nobody can come and cut off your hair while you are sleeping and sell it for wigs. It is not legal for them to *"look like"* they are asking for your permission, if they do so in a manner meant to confuse you.

GOOGLE

"Data-rape" **should not be ok with you**. You get pulled into the big party known as "the internet" like a Frat House rumble because "*everybody is doing it*". You are slipped some movies and MP3's and fake dating profiles to get you "*loosened up*". Then, when your defenses are down, in this unfamiliar place called the internet, your most private thing is taken from you: **Your privacy itself.**

A precedent exists for the compensation of individuals for the selling of any part of their body (Blood banks, semen banks, kidney exchanges, etc.) , time (W2 Employment), expertise (1099 Consulting), brand (Celebrity endorsement), persona (Online **Vlog** subscriber promotions) and a host of other past examples proving the value precedent of personal humanity.

The concept of ownership of your private data is the basis of multiple class-action lawsuits in development against privacy-violation and data exploitation efforts akin to the home mortgage issues. Disclosures that are hidden or written in language that is incomprehensible to the average person, don't count! In tests: 20, unexpectedly picked, people are asked to read the website disclosures for a dot.com company in the few seconds they are allowed to read it (the average time that web metrics says the average user is exposed to the disclosure) and scroll through the massive amount of legalese and comprehend it. Not one of them could answer 10 follow-up questions about what it said. Try it yourself with 20 friends. This sort of test will be a key evidence point in the trials.

Why did the privacy heads at top big internet companies like Google and Twitter quit just before the Snowden disclosures?

Companies like Facebook and Google make billions of dollars, almost entirely, off of the selling of your personal information, why shouldn't you share in the money they make off of you without your fully informed consent? Send Twitter a bill for using you, if they don't pay you, you have a legal right to collect. At least one, of the many cases underway, will prevail. Then, every time you use anything on Google, you get a check, from Google, for that part of yourself that was used by them.

Interesting concept!

Watch what comes next...

Weston L.- NY T

Facebook Sued Over Alleged Scanning of Private Messages

Facebook Inc. (FB) was sued over allegations it systematically intercepts its users private messages on the social network and profits by sharing the data with advertisers and marketers. When users compose messages that include links to a third-party website, Facebook scans the content of the message, follows the link and searches for information to profile the message-sender's Web activity, violating the Electronic Communications Privacy Act and California privacy and unfair competition laws, according to the suit.

The practice compromises privacy and undermines Facebook's promise of "unprecedented" security options for its messaging function, two Facebook users said in the complaint filed in federal court in San Jose, California.

Lawsuits against Internet companies and social networks are multiplying as use of the Web balloons and users become more aware of how much personal information they're revealing, often without their knowledge. Google Inc. (GOOG), Yahoo! Inc. and LinkedIn Corp. (LNKD) also are facing accusations of intercepting communications for their profit at the expense of users or non-users.

'Invasive Scanning'

The scanning "is a mechanism for Facebook to surreptitiously gather data in an effort to improve its marketing algorithms and increase its ability to profit from data about Facebook users," Michael Sobol, an attorney for the plaintiffs, wrote in the Dec. 30 complaint.

Photographer: Daniel Acker/Bloomberg

When users compose messages that include links to a third- party website, Facebook... Read More

Jackie Rooney, a spokeswoman for Facebook, said the company regards the allegations as "without merit."

The plaintiffs are seeking a court order certifying the case as a group, or class action, lawsuit on behalf of all Facebook users who have sent or received a private message in the past two years that included a Web links. They are also asking to bar Facebook from continuing to intercept messages and seek as much as $10,000 in damages for each user.

The case is Matthew Campbell v. Facebook Inc., 13-5996, U.S. District Court, Northern District of California (San Jose).

To contact the reporter on this story: Karen Gullo in federal court in San Francisco at kgullo@bloomberg.net

To contact the editor responsible for this story: Michael Hytha at mhytha@bloomberg.net

----

Reporters- For follow-up information on privacy data lawsuits:

Chris Hansen, Senior National Staff Counsel- ACLU- 212-549-2500

Eric Gibbs, Founding Partner- Girard Gibbs LLP - 1-866-981-4800

Elizabeth Fegan- Partner- Hagens Berman- 1-206-623-7292

Ryan D. Andrews- Edelson, LLC- (312) 589-6370

Seanna R. Brown- Baker Hostetler - 212-589-4230

More coming...

The Internet Privacy Warrant Association Campaign

WARRANT

The IPWA is an independent association of writers, publishers, reporters, citizens and families. Signatories are allowed to post the trust, icon, above, on their websites. Signatories must link the icon, above, to an exclusively dedicated page on their website with a color scan of the original CEO-signed warrant (in blue text, below) on their letterhead. **Disclosure:** IPWA is not a front organization for a billionaire. IPWA does not accept funds. IPWA is just people with families. IPWA does not support any candidate.

HERE IS THE BEST AND EASIEST PART FOR THESE BIG COMPANIES: Just do it! You don't need to send anything in to IPWA or apply or, anything. **Just do it** and make sure it is the truth. **Everybody is watching**. If you don't do it, everybody will know. If you do do it, everybody will know. If you do it and lie, everybody will know. IWPA has written all of the companies, on the list below, asking them to do it. There are no membership fees to pay. There is no ongoing "certification service cost". It is totally free. **Just do it** and make sure it is the truth! **Everybody is watching! Don't change the wording in blue, not even one letter, or everyone will know you are using "sneaky-talk".**

We ask each company selling services online, or services related to online use, to sign the following warrant and guarantee. **If you are a consumer, or a consumer support group, cut-and-paste a copy of this article and email it to any email address you have, for people at the companies on the list below to help keep them motivated. You might want to not shop at, or cancel your subscription to, those companies below, until they sign up.**

It is not a "promise". A "promise has no bearing under law. This is a legally binding agreement and statement of trust:

WARRANT AND GUARANTEE OF ________ (COMPANY___________

"As CEO, and as the legally bound representative for _____________ (COMPANY) I, and my company, warrant and guarantee that our company is not providing access to hackers, bulk privacy harvesting groups or any similar third parties who may abuse your privacy data rights."

NAME:
CEO, _________________________(COMPANY)________________
Signature:
Date:
Company:
Address:
Phone:
Fax:
Email:
########

The Following Companies either have not signed the warrant, or have not responded to requests to sign the warrant, and thus, may be intentionally, or negligently, delivering your data to hackers and bulk privacy harvesting companies:

Amazon.com
Match.com
Okcupid.com
Google.com
Twitter.com
Facebook.com
Linkedin.com
Level 3
AT&T

Sprint
Verizon
Radio Shack
Adobe
Comcast
Apple
Ebay
Priceline.com
Rakuten
Macy's
Yahoo.com
Baidu.com
Salesforce.com
Microsoft
Intel
NVIDIA
Target
Walmart
Costco
Safeway
Walgreens
CVS

Additional names to be added...

Peter Lesting- Associate- IPWA
Dean Unsen- Associate- IPWA

Reports from Der Spiegel and ABC now reveal that:

1. If you ever expressed any negative thoughts or words about a Senator, political group or business monopoly it was documented on Amazon's Cloud servers and you get "flagged".

2. Amazon hosts the servers for bulk data privacy harvesting groups where the log of your name being "flagged" for mouthing off ends up.

3. If you order anything from Amazon that is electronic, it gets stopped, on its way to you, bugs and spyware are inserted in the cord, chips or hard-drive and it is sent along to you.

Amazon hosts Netflix and grabs some of Netflix viewers watching habits and profiling data for "marketing purposes", as well. Currently there are no interstitial latent images dropped into Netflix streams but the technology to do so has been tested repeatedly.

Sooooooooo... **don't "mouth off".**

SD-ABC

Read about how you get "DATA-RAPED" here...

[caption id="attachment_8591" align="aligncenter" width="529"] Read about how you get "DATA-RAPED" here...[/caption]

Google, once disdainful of lobbying, now a master of Washington influence

Google's Eric Schmidt is no stranger to D.C. He has spent lots of time at the White House and on Capitol Hill lobbying on behalf of his titan technology company. But his relationship with Washington and the Obama administration has not always been a comfortable one.

Written by [Tom Hamburger Matea Gold]

Published: April 12

E-mail the writers

In May 2012, the law school at George Mason University hosted a forum billed as a “vibrant discussion” about Internet search competition. Many of the major players in the field were there — regulators from the Federal Trade Commission, federal and state prosecutors, top congressional staffers.

What the guests had not been told was that the day-long academic conference was in large part the work of Google, which maneuvered behind the scenes with GMU’s Law & Economics Center to put on the event. At the time, the company was under FTC investigation over concerns about the dominance of its famed search engine, a case that threatened Google’s core business.

In the weeks leading up to the GMU event, Google executives suggested potential speakers and guests, sending the center’s staff a detailed spreadsheet listing members of Congress, FTC commissioners, and senior officials with the Justice Department and state attorney general’s offices.

“If you haven’t sent out the invites yet, please use the attached spreadsheet, which contains updated info,” Google legal assistant Yang Zhang wrote to Henry Butler, executive director of the law center, according to internal e-mails obtained by The Washington Post through a public records request. “If you’ve sent out the invites, would it be possible to add a few more?”

Butler replied, “We’re on it!”

On the day of the conference, leading technology and legal experts forcefully rejected the need for the government to take action against Google, making their arguments before some of the very regulators who would help determine its fate.

The company helped put on two similar conferences at GMU around the time of the 18-month investigation, part of a broad strategy to shape the external debate around the probe, which found that Google’s search practices did not merit legal action.

The behind-the-scenes machinations demonstrate how Google — once a lobbying weakling — has come to master a new method of operating in modern-day Washington, where spending on traditional lobbying is rivaled by other, less visible forms of influence.

That system includes financing sympathetic research at universities and think tanks, investing in nonprofit advocacy groups across the political spectrum and funding pro-business coalitions cast as public-interest projects.

The rise of Google as a top-tier Washington player fully captures the arc of change in the influence business.

Nine years ago, the company opened a one-man lobbying shop, disdainful of the capital’s pay-to-play culture.

Since then, Google has soared to near the top of the city’s lobbying ranks, placing second only to General Electric in corporate lobbying expenditures in 2012 and fifth place in 2013.

The company gives money to nearly 140 business trade groups, advocacy organizations and think tanks, according to a Post analysis of voluntary disclosures by the company, which, like many corporations, does not reveal the size of its donations. That’s double the number of groups Google funded four years ago.

This summer, Google will move to a new Capitol Hill office, doubling its Washington space to 55,000 square feet — roughly the size of the White House.

Google’s increasingly muscular Washington presence matches its expanded needs and ambitions as it has fended off a series of executive- and legislative-branch threats to regulate its activities and well-funded challenges by its corporate rivals.

Today, Google is working to preserve its rights to collect consumer data — and shield it from the government — amid a backlash over revelations that the National Security Agency tapped Internet companies as part of its surveillance programs. And it markets cloud storage and other services to federal departments, including intelligence agencies and the Pentagon.

“Technology issues are a big — and growing — part of policy debates in Washington, and it is important for us to be part of that discussion,” said Susan Molinari, a Republican former congresswoman from New York who works as Google’s top lobbyist. “We aim to help policymakers understand Google’s business and the work we do to keep the Internet open and spur economic opportunity.”

Molinari added, “We support associations and third parties across the political spectrum who help us get the word out — even if we don’t agree with them on 100 percent of issues.”

Susan Molinari, a Republican former congresswoman from New York, works as Google’s top lobbyist in Washington.

As Google’s lobbying efforts have matured, the company has worked to broaden its appeal on both sides of the aisle. Executive Chairman Eric Schmidt is a well-known backer of President Obama and advises the White House. Google’s lobbying corps — now numbering more than 100 — is split equally, like its campaign donations, among Democrats and Republicans.

Google executives have fostered a new dialogue between Republicans and Silicon Valley, giving money to conservative groups such as Heritage Action for America and the Federalist Society. While also supporting groups on the left, Google has flown conservative activists to California for visits to its Mountain View campus and a stay at the Four Seasons Hotel.

The company has also pioneered new and unexpected ways to influence decision-makers, harnessing its vast reach. It has befriended key lawmakers in both parties by offering free training sessions to Capitol Hill staffers and campaign operatives on how to use Google products that can help targetvoters.

Through a program for charities, Google donates in-kind advertising, customized YouTube channels and Web site analytics to think tanks that are allied with the company’s policy goals.

Google “fellows” — young lawyers, writers and thinkers paid by the company — populate elite think tanks such as the Cato Institute, the Competitive Enterprise Institute and the New America Foundation.

To critics, Google’s investments have effectively shifted the national discussion away from Internet policy questions that could affect the company’s business practices. Groups that might ordinarily challenge the policies and practices of a major corporation are holding their fire, those critics say.

“Google’s influence in Washington has chilled a necessary and overdue policy discussion about the impact of the Internet’s largest firm on the future of the Internet,” said Marc Rotenberg, a Georgetown University law professor who runs the Electronic Privacy Information Center, a watchdog and research organization.

Some with deep ties to the company say that Google’s embrace of aggressive lobbying was a necessary concession to the realities of Washington.

“I don’t fault Google for playing that game, in which big companies use their money to buy advocates and allies,” said Andrew McLaughlin, who served as Google’s first director of global public policy in Washington. “Given where the company is today, the fiduciary duty it has to shareholders and the way Washington works, it’s a rational judgment.”

Google goes to lunch

An early sign of Google’s new Washington attitude came in September 2011, when executives paid a visit to the Heritage Foundation, the stalwart conservative think tank that has long served as an intellectual hub on the right, to attend a weekly lunch for conservative bloggers.

The session took place at a critical juncture for the company.

Days earlier, Schmidt had endured a rare and unnerving appearance on Capitol Hill, where he was lectured by a Republican senator who accused the company of skewing search results to benefit its own products and hurt competitors. The FTC antitrust inquiry was underway. And, in what Google saw as a direct threat to the open Internet, major lobbies such as the U.S. Chamber of Commerce and the Motion Picture Association of America were mounting a legislative campaign to place restrictions on the sale of pirated music and movies. The effort was getting bipartisan traction in the House and the Senate.

Google Executive Chairman Eric Schmidt testifies before a Senate Judiciary antitrust subcommittee in September 2011. (Chip Somodevilla/Getty Images)

Inside Google’s Washington headquarters, a handful of lobbyists were crafting what they called the “Republican strategy” to defeat the legislation. Their approach: build conservative opposition based on the right’s distaste for regulation. They also seized on an obscure provision that they told Republicans would be a boon for trial lawyers, a Democratic constituency.

As the campaign took shape, there was a building sense within the company that it needed to beef up its firepower on the Hill. That fall, Google’s first Washington lobbyist, a computer scientist and lawyer named Alan Davidson, a Democrat, would announce his resignation, replaced a few months later by the former GOP lawmaker, Molinari.

In their visit to Heritage that day, Google officials were eager to make new friends. Their challenge was instantly clear.

“In 2008, your CEO campaigned for Barack Obama,” said Mike Gonzalez, Heritage’s vice president for communications, according to a video of the event. “. . . As a company, you’re really identified with this administration from the beginning. And you come here and you’re like a mix of Milton Friedman and Friedrich Hayek.”

Adam Kovacevich, then a member of Google’s policy team, responded by stressing the company’s interest in building new alliances.

“One of the things we’ve recognized is that no company can get anything done in Washington without partnerships on both sides of the aisle,” he said.

He noted the recent hiring of Lee Carosi Dunn, one of several former top aides to Sen. John McCain (R-Ariz.) brought on by the company.

Dunn, addressing the audience, promised “a lot of reach-out to Republicans.”

“I think it’s another lesson young companies that come to Washington learn — you can’t put all your marbles in one basket,” Dunn said. Referring to the editor of the conservative Weekly Standard, Dunn added: “Look, even Bill Kristol was walking around wearing Google glasses. We’re making strides!”

The Google-Heritage relationship soon blossomed — with benefits for both.

A few weeks after the blogger session, Heritage researcher James L. Gattuso penned a critique of the antitrust investigation into Google, praising the company as “an American success story.”

That winter, Heritage joined the chorus of groups weighing in against the anti-piracy legislation. As the bill, the Stop Online Piracy Act, appeared to gain steam in the GOP-led House, Gattuso wrote a piece warning of “unintended negative consequences for the operation of the Internet and free speech.” The legislation, he said, could disrupt the growth of technology. Gattuso said he came to his position independently and was not lobbied by Google.

After Gattuso’s piece went live, Heritage Action, the think tank’s sister advocacy organization, quickly turned the argument into a political rallying cry. In terms aimed at tea party conservatives, the group cast the bill as “another government power grab.”

In mid-January 2012, Heritage Action designated the legislation a “key vote” it would factor into its congressional race endorsement decisions — heightening the pressure on Republicans.

The next day, leading Internet sites, including Wikipedia, went dark as part of an online blackout protesting the bills.

Google turned its iconic home page into a political platform for the first time, urging users to sign a petition against the legislation. Seven million people added their names, and many of them added their e-mails, creating a valuable activist list for Google to mobilize then and in later fights.

As congressional offices were flooded with phone calls and e-mail protests, support for the legislation crumbled. Within days, both the House and Senate versions of the bill were shelved and Hill veterans were left marveling at the ability of Google and its allies to muster such a massive retail response.

For Google and Heritage, the legislative victory was the beginning of a close relationship. A few months later, Google Ideas and the Heritage Foundation co-hosted an event focused on the role the Internet could play in modernizing Cuba, featuring Sen. Marco Rubio (R-Fla.) and Google Ideas director Jared Cohen.

The following year, a new name popped up on Google's list of groups it supports financially: Heritage Action.

GMU conferences

Facing a broad and potentially damaging FTC probe, Google found an eager and willing ally in George Mason University's Law & Economics Center.

The center is among the academic programs at universities such as Harvard and Stanford that have benefited from Google's largesse. For the past several years, the free-market-oriented law center has received an annual donation from the company, a grant that totaled $350,000 last year, according to the school.

Google's relationship with the law center proved helpful in the summer of 2011 as speculation mounted that the FTC was going to launch an antitrust investigation of the tech giant. The company's rivals, including Microsoft and Yelp, were aggressively pressing arguments that Google was exploiting its dominance in the search business.

On June 16, 2011, Google and the law center put on the first of three academic conferences at the GMU law school's Arlington County campus, all focusing on Internet search competition. It was eight days before the company announced it had received formal notification it was under FTC investigation.

Google was listed as a co-sponsor of the day-long forum, but some participants were still struck by the number of speakers who took a skeptical view of the need for antitrust enforcement against the company, according to people in attendance.

The keynote address was by Google engineer Mark Paskin, who delivered a lunchtime speech titled "Engineering Search."

A few days later, Christopher Adams, an economist in the FTC's antitrust division who later worked on the Google investigation, e-mailed Butler, the law center's director, to thank him for putting on the conference. "I think it was one of the best policy conferences that I've been too [sic]," Adams wrote, praising Paskin's talk as "excellent."

Adams declined to comment for this article, referring questions to the FTC press office.

FTC spokesman Justin Cole said the agency's staffers "are required to adhere to established federal government ethics rules and guidelines. Attendance and participation in the 2011 and 2012 GMU conferences by our staff adhered to these guidelines."

As the agency's investigation stretched into its second year, the staff and professors at GMU's law center were in regular contact with Google executives, who supplied them with the company's arguments against antitrust action and helped them get favorable op-ed pieces published, according to the documents obtained by The Post.

The school and Google staffers worked to organize a second academic conference focused on search. This time, however, Google's involvement was not publicly disclosed.

Months before the event, Zhang, the Google legal assistant, e-mailed Chrysanthos Dellarocas, a professor in the Information Systems Department at Boston University's School of Management, to suggest he participate. Dellarocas had received $60,000 in 2011 from Google to study the impact of social networks on search.

"We'd love for you . . . to submit and present this paper, if you are interested and willing," she wrote.

When GMU officials later told Dellarocas they were planning to have him participate from the audience, he responded that he was under the impression from "the folks at Google who have funded our research" that they wanted him to showcase his work at the event. He said he wanted "to be in compliance with our sponsor's expectations."

Dellarocas, who had a schedule conflict and ultimately did not attend, told The Post that while Google occasionally checked on his progress, the company did not have any sway over his research.

"At no point did they have any interference with the substance of my work," he said.

Even as Google executives peppered the GMU staff with suggestions of speakers and guests to invite to the event, the company asked the school not to broadcast its involvement.

“It may seem like Google is overwhelming the conference,” Zhang fretted in an e-mail to the center’s administrative coordinator, Jeffrey Smith, after reviewing the confirmed list of attendees a few weeks before the event. She asked Smith to mention “only a few Googlers.”

Smith was reassuring. “We will certainly limit who we announce publicly from Google,” he replied.

A strong contingent of FTC economists and lawyers were on hand for the May 16, 2012, session, whose largely pro-Google tone took some participants aback. “By my count, out of about 20 panelists and speakers, there were 3$^{1}/_{2}$ of us who thought the FTC might have a case,” said Allen Grunes, a former government antitrust lawyer who served on a panel and described the conference as “Google boot camp.” Grunes said he was not aware of Google’s role organizing the event until informed of it by a Post reporter.

Daniel D. Polsby, dean of GMU’s School of Law, which houses the center, said that while Google provided suggestions, the agenda and speakers were determined by university staffers. “I think it would misrepresent this conference to suggest that it was a Google event,” he said, adding that the law center discloses on its Web site the support it gets from Google and other corporations.

Google declined to comment about the conferences.

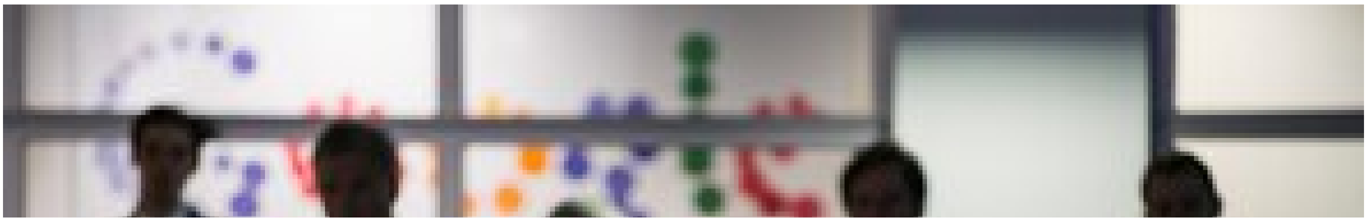
In January 2013, after an investigation that spanned more than a year and a half, the FTC settled the case with Google, which agreed to give its rivals more access to patents and make it easier for advertisers to use other ad platforms.

But when it came to the charges that Google biased its search results to promote its own products, the five FTC commissioners all voted to close the investigation, saying there was no evidence the company’s practices were harming consumers.

Jon Leibowitz, then the chairman of the agency, said in an interview that the FTC was not affected by Google’s campaign, noting that the company’s rivals were waging a parallel effort on the other side.

“It didn’t bother me that a lot of people were building events around the possibility of the FTC investigation,” said Leibowitz, who has since left the FTC. “That’s sort of life in the big city, and both sides were doing it.”

Sen. Marco Rubio (R-Fla.) discusses the U.S. economy in a March speech at a Jack Kemp Foundation forum at Google’s Washington offices. (T.J. Kirkpatrick/For The Washington Post)



Attendees listen to Rubio’s speech. While also supporting groups on the left, Google has courted conservative groups and lawmakers in recent years. (T.J. Kirkpatrick/For The Washington Post)

NSA fallout

On a February night this year, Schmidt sat down with a Washington audience far friendlier than the panel of senators who had grilled him nearly three years earlier. Addressing a dinner of journalists and scholars at the libertarian Cato Institute, Schmidt received applause and lots of head-nodding as he declared, “We will not collaborate with the NSA.”

Cato was not always in sync with Google’s policy agenda. In previous years, the think tank’s bloggers and scholars had been sharply critical of the company’s support for government rules limiting the ways providers such as Comcast and Verizon could charge for Internet services.

But, like manyinstitutions in Washington, Cato has since found common ground with Google.

And the think tank has benefited from the company’s investments, receiving $480,000 worth of in-kind “ad words” from Google last year, according to people familiar with the donation.

Schmidt’s message to Cato that night in February reflected the current focus of Google’s energy — containing the fallout from revelations by NSA leaker Edward Snowden.

As the public’s outrage has grown, the tech giant has tried to keep the focus on limiting government surveillance, not on the data collection done by private companies. A White House review of those issues is expected to be released this coming week.

A campaign against government spying, meanwhile, is in high gear, drawing together some unexpected bedfellows. The American Civil Liberties Union, Heritage Action, Americans for Tax Reform and the Center for Democracy & Technology have formed a coalition calling for the government to obtain a probable-cause warrant before getting access to e-mails and other electronic data.

The coalition, Digital 4th, is funded by Google.

Alice Crites contributed to this report.

Tens of thousands of Fake profiles on big dating sites are there to suck in your marketing data, MORE HERE>>>

Big "Famous" Search Engines exist to tell you what THEIR backers want you to know, NOT what you want to find!

All of the big well-known search engines (google, Ask, Bing, etc.) are now operated by special interest groups and bulk data harvesting conglomerates who have modified the algorithms to steer the perspectives they want you to have at you, and not the information you want to find.

They cut our candidates, policy issues and competitors that they are against and emphasize those that they support in the search results.

The creation of digital sheep is a subtle process of steering their points of view to the first bunch of response pages and burying perspectives, that they don't want you to get, to 20 pages back. Spy agencies say that any average person can be brainwashed in 5 days with "effective techniques". Compromised search engines are VERY "effective techniques".

If you must use a "main stream" search engine, click on pages 15, or later first, for any hope of getting fair research.

A number of start-ups and university groups are working on 100% unbiased search engines that will agree to warrant and guarantee zero-manipuation but they are not fully online yet.

When you you type in the manipulated search engines, you are just asking them to:

- Archive your interests and personality type.
- Sell you stuff based on their privacy harvesting of your personal information.
- Come up with search results that slowly start to get you think like their financial backers also think.
- Avoid showing you search results that conflict with the interests of their financial backers.

It is virtually impossible to now find a database that has not been hacked into multiple times, mostly by bored 14 year olds. Current network hardware is full of archaic "back-doors" and current software for networks is as secure as your cookie jar.

Isn't the internet wonderful?
JK-LAT, GH- NYT

Two great hacker protection articles:

http://m.nbcnews.com/technology/how-protect-your-internet-privacy-2014-2D11762947

https://pressfreedomfoundation.org/encryption-works#pgp

Cisco's Last Hope!

The NSA disclosures have put Cisco at risk of extreme, or total, failure. Cisco's marketing, branding and market analytics experts will not have accurate reports completed on this, for Cisco for months. BY then it will be too late.

In order for Cisco to recover from the damage it needs to, this week, announce that all hardware will be "open source certified" by the open source community and that a new serial number series will begin the verification process. Existing hardware, which the open source community finds to be back-door-free will receive upgraded serial number designations. Problem solved!

TDG- LAT

Personal Privacy Security 2014:

(What a drag...)

- Get rid of your credit cards. Only use cash.
- Tape over every digital camera lens. Don't buy devices with built-in cameras.
- Unplug both the power cord and network cord of any device that network connects, when not in use. Routers, gamebox, appliances, Smart TV's, etc. They all watch you.
- Never leave your wifi unit in the "on" position.
- Keep your cell phone in "flight" mode or "airplane" mode until you are ready to use it and then turn it off after use.
- Always remove the battery from your phone when you go into a meeting or drive between locations.
- Try to buy devices that do not have a GPS chip in them.
- Don't "sync" any device.
- Phone, computer and other wall charger/adapters often have bugs built into them.
- Delete your contact list, calendar, tasks & memos from any mobile device. Carry them on paper or on a device with no modem, wifi or bluetooth.
- Never use a "social network" site. Delete all data and cancel all existing sites.
- Remember: "If it has a plug, it has a bug".
- Use TOR and peer to peer hardware and software certified by the open source community.
- Never post your picture online. If you do, make sure it is only used once per site and has your own steganography ID in it but your data meta tags stripped out.
- Don't own anything with an RFID chip. Even your car tires have them in them.
- Cover your mouth when saying something important. Surveillance cameras read lips.
- Don't keep anything of value on a network-connected hard drive or server. Use only external drives, encrypt them and unplug them when not in use.--

Who is fixing the hacking crisis?

Russian mobster hackers, Chinese corporate espionage teams, Mexican cartel technologists, teenage competitive break-in coders and a host of others are after your stuff. They are coming all day and all night.

How do we sleep at night now that we know that our business plans, our engineering CAD for our new products, our publishers book manuscripts, our trade secret formula's, our marketing plans and, essentially, our every thought and business idea is up for grabs on every phone and device we own?

Have hope. The next generation of solutions are on their way.

A wave of innovators are bringing the solutions to market soon. The open source community is coming to save you.

Part of the effort has delivered Peer-to-peer self creating, self-erasing mobile and desktop networks. These cell phone networks bypass cell phone towers, are untraceable and move so mercurially that once they are found, they dissolve into nothing. They run entirely off of software and need no special chips. They cannot be tracked or spied on. (Tor, Onion, Mega, Serval, McAfee, T5, Torrents, Gnutellas, Freewire, Darkmail, Roofnet, and hundreds more)

New operating systems that are created and monitored by the open source community ensure that the creators of spying and the suppliers of hackers tools are no longer the same people.

One phone company has been forced out of the market for having spy chips and others are sure to follow. New, independent handset projects will deliver cell phones that can use a variety of Operating Systems (OS) and that have all of their chips and circuit diagrams publicly logged for any open source participant to validate and confirm that no hidden spy chips exist within.

Hundreds of start-ups, programming teams, public projects, kickstarter/IndieGoGo, efforts, individual coders and large commercial efforts are engaged in delivering these solutions to solve the current crisis of confidence in the tech sector. While Nokia and old school players promote their party line: "none of these technologies will work", they see the writing in the wind, they know that they DO work, and they know that they must play or go away.

TD- IT Wire

DEVELOPING STORY: Consumer groups demand assurances that Microsoft Outlook and Apple iCal Calendars are not sending your schedule, contacts, tasks and memos off your machine, or device, to third parties.

FG-, GH, PP-NYT

The Amazing Gift of the Public Spying Scandal:

There are some great things coming out of it -
A. Transparency

B. Free diary management service

C. Validation that online voting CAN now work because we now know that nobody can actually cheat it. In fact, you may have already voted because they already know what you are thinking! Cool right?

D. Free lifetime personal autobiography services and archiving provided by your tax dollars.

E. Inability to actually get defrauded by online sales because we now know they can track down ANY bad guy!

----

http://www.youtube.com/watch?v=ymkA1N3oFwg

Can You Hack It?
Everything electronic you own—iPhone to subway card to power strip—can be hacked. So how to defend yourself.

By Amy Webb For Slate.com

Wherever you're sitting right now, take a moment to note the connected devices around you. In your pocket or handbag, you probably have an electronic key fob and perhaps a rechargeable subway card embedded with RFID. You likely have a smartphone, which is connected to a Wi-Fi network and also has voice-mail service.

You might be wearing a Nike FuelBand, or a Fitbit, or possibly even a new pair of Google Glass. Maybe you can spot a traffic light or an orange highway sign out of your window. A power strip is likely not too far away.
All of these devices share one thing in common: They can be hacked.

As we herald the coming Internet of Things, it's easy to forget that our ever expanding tech playground is mostly unsupervised. There is no playground teacher to blow a whistle when another kid takes control of your Bluetooth headset. There is no Norton antivirus software for your garage door opener. If you can plug it in or connect it to a network, your device—no matter what it is —can be harnessed by someone else. And that someone doesn't have to be a Chinese superhacker to do some serious damage with it, either on purpose or by accident. It can be your Uncle Roger, who doesn't have his new iPhone figured out and is cluelessly turning your lights on and off via your Belkin WeMo.I'm a hobbyist. Because I study emerging technlogy and the future of media, I'm often tinkering, breaking things, and putting them back together. Once, I wanted to see if I could break into the protected Wi-Fi network we set up for my daughter at home. Less than an hour later, I'd failed to penetrate her network but managed to shut down the main network for our house. Which I knew, because of my husband's sudden yelling upstairs: "Why is the IRS website redirecting to Sesame Street?!"Part of what makes new technology so exciting is that, unlike the old days, it works right out of the box.

You no longer need to know how to build a computer, connect a modem, run a terminal emulator, and install bulletin board system, or BBS, software in order to send a racy message to a co-worker. Now any tech idiot can download Snapchat and accidentally send a racy photo to his sister-in-law. The tech playground is more accessible and, as a result, increasingly problematic.Just after the annual Black Hat Internet security convention a few months ago in Las Vegas, I asked a group of my friends—a Navy engineer, a professional hacker, and a hobbyist—to help me come up with a quick list of devices that will be vulnerable during the next few years as the Internet of Things becomes widespread.

Here's our (incomplete) list. (Entries with a * are those we've tried hacking at home, for fun.):Obvious- smartwatches*; smartphones*; computers*; tablets and phablets*; home computer locks*; the cloud (services, storage, software); ATMs at banks; printers; GPS devices*; Wi-Fi routers*; webcams*; thumb and portable USB drives; hotel and gym safes (they tend to use a single default passcode); cable box or DVR; voice mail (especially those with a global call-in number that doesn't lock outafter successive failed attempts—we saw this with the News of the World scandal); Less Obvious- power strips (can be infected with malware); power cords for your devices (code can be implanted); luggage trackers (such as the Trakdot); connected glasses (Google Glass, Oculus Rift. As of now, Google's QR barcodes for Wi-Fi store the full access point name and password as plain text); gaming consoles: PS3, Kinect, Nintendo*; refrigerators (such as Samsung); cars with computer operating systems; smart pens (like the Livescribe); gesture control devices (such as the Leap)*; SD cards; cameras; smart alarm clocks*; coffee makers; key fobs; light switches*; moisture sensors*; kitchen and pantry trackers (such as Egg Minder); insurance driving monitors, such as Progressive's Snapshot device'; traffic lights (MIRT transmitters can change lights to green in two to three seconds); highway signs that spell out text;

...And we didn't even get into medical devices, which are frighteningly exposed to mischief.The proliferation of all this technology creates a constant need to keep devices updated and secure. Perhaps the most vulnerable object in any American house is the cable box, because it is so rarely updated.

If what I'm saying makes you uneasy, you're not alone. There are plenty of new products exploiting the fears of techno-theft, promising to keep you locked down and safe, such as this neck security wallet from REI, which says it'll block criminals from scanning the RFID chip in your passport. I travel to a lot of different countries every year for work. I've had zero attacks on my passport. On the other hand, I've had two laptops and an iPhone compromised.So how should we think about our constant vulnerability? I make a daily assumption that everything I do is hackable, but almost nothing I do is worth hacking. I have an awareness of potential vulnerabilities, and I'm trying to develop an evolving set of street smarts. You should, too.For example, since I do a lot of work on the road while I travel, I now carry my own Wi-Fi hotspot. I can use a secure virtual private network to send and receive email and to access content that I have stored in the cloud. (To be sure, that network can be hacked, too, but at least I can watch the logs of what's coming and going and attempt to fight off intruders.)I also keep this network cloaked, meaning that I haven't named it "Amy Webb's Hotspot."

I routinely look at networks, just for fun, and I'm astonished at how many people use their own names or the names of their companies. Instead, I've changed the names of all of my devices to my mobile phone number. That way, if my laptop is lost or stolen, someone will see a phone number rather than my name, which I hope means there will be less of an incentive to poke around my machine to see what's there.

My passwords are easy to remember but difficult to crack. According to my hacker friend, you're best off with a long phrase that also includes numbers and at least one capital letter. Something like "Iwant99pizzasand12beersfordinnertonight" is actually more secure than "Gx1U2y," because the algorithms that are used to crack passwords have to process many more computations the longer a password is, and as of now they're mostly not using natural language processing. Speaking of passwords, I change them weekly. It should go without saying that each one of your networks and devices should have a different password. When was the last time you changed yours?

Because I know you're wondering: There is no workaround for this and no way to game the management of your own passwords.Another good rule is to turn off your peripherals when they're not in use.

Don't leave your nanny cam on all day long. Same goes for non essentials on your network, such as additional computers, game consoles, and the like. The more things you have plugged in, the more opportunities there are for penetration. Be cognizant of who's plugging what into your network and connected devices. An innocent-looking thumb drive can destroy your computer within seconds. I'm not preaching abstinence here, but I am saying that computer viruses can be as menacing as sexually transmitted diseases: invisible to the naked eye, but most of the time totally preventable with the right precautions taken in advance.More importantly, I'd argue that all this hacking isn't necessarily a bad thing. A lack of rules is actually helpful for our burgeoning Internet of Things. I'd much rather that we all come to a good understanding of how our machines work than to start imposing regulations and restricting access.

Sometimes, a collaborative hacking effort yields beneficial results for all. For example, the city of Philadelphia launched a contest and invited hackers to create apps and widgets to help citizens receive updates on emergencies and city news and to contact city administration. During Superstorm Sandy, Philly311 was the 33rd most-downloaded app in the country. The city since partnered with Random Hacks of Kindness and Code for America to bring local hackers together with residents, share knowledge, and build more resources.The tech playground is open to all, offering a fantastic opportunity to teach kids how to use and control the many devices that are inextricably tied to their futures. The more they break, the more they'll learn how to collaborate, fix, and innovate. Organizations like SparkFun Electronics are using next-generation open- source code to show everyone how to build and hack our Internet of Things.

Open networks are vital to innovation, even if they aren't totally secure. Personally, I'm looking forward to 50 years from now when I think the wrong sequence while looking at the light fixture in my grandchild's house and accidentally cause a blackout. China will offer to sell any journalist a whole set of transcripts from this, and other scandals.

The COMPLETE LIST Update:

"If it has a plug, it has a bug!"

Hackers from every country, bored children with any computer, any spy, any ex lover with a computer, any business competitor and anybody who wants to, can hack via these doorways. By now, most of America has seen the network TV Series: ***"Person of Interest"*** ; thus, nothing on this list should be a big surprise, to most people. Every one of the items on this list has now been documented, as hacked, in widely available public media:

- Everything you buy on **Amazon.com**; your locations, addresses, credit cards, sizes, preferences. (Amazon provides the servers for the spy agencies, per **60 Minutes.** 60 Minutes says Amazon is even planning to **"drone you".**)
- Everything you buy from any online retailer including your locations, addresses, credit cards, sizes, preferences.
- Any porn you download or watch off any server.
- Everything you watch on **Netflix**, **Hulu**, **VuDu**, and any online media service including the times you watched, your preferences and every title you ever ordered.
- Smartwatches
- Anything that you log into with a single user name and a single password. Criminals throw high-speed computers at it and they eventually try every combo until they get in.
- Smartphones
- Computers
- **Cisco** Products. Security Backdoors were built into them that criminals have now accessed.
- **Netgear** Products. Security Backdoors were built into them that criminals have now accessed.
- Tablets and phablets
- Utility **SmartMeters** report when you are home, or not, by when you turn things on and off and they may be hackable by programmers to provide other feeds about you.
- Home computer locks
- The cloud (services, storage, software) **Amazon Cloud**, **SkyDrive**, **Box**, **Drop Box**
- ATMs at banks
- WiFi printers
- Baby monitors
- **Twitter** accounts
- **T-Mobile** accounts
- **Adobe** accounts
- **AT&T** accounts
- **Google** accounts
- **Facebook** accounts
- GPS devices
- Wi-Fi routers
- Webcams
- Any of your locations, buying habits, preferences, use periods or related data captured by any device on this list
- Thumb and **portable USB** drives
- **Hotel and gym safes** (they tend to use a single default passcode)
- **Cable** box or DVR
- Voice mail
- **Target, Costco, Walmart** credit card readers
- In **car bluetooth hands-free** microphones
- Any **bluetooth** connections
- **Google** Cookies or ANY cookies that your browser accepts
- Any infra-red port on a device
- **Power strip**s (can be infected with malware)
- Power cords for your devices (code can be implanted)
- Luggage trackers (such as the **Trakdot**)
- **Keyfinders** or electronic finder tags
- Grocery store discount cards: **Safeway**, **Albertsons**, **Walgreens**, **CVS**, etc.
- Connected glasses (**Google Glass**, **Oculus Rift**. As of now, **Google's** QR barcodes for Wi-Fi store the full access point name and password as plain text)
- Gaming consoles: **Playstation**, **Kinect**, **Nintendo**
- Smart refrigerators (such as Samsung)
- Cars with computer operating systems- **Siri**, **MS Sync**, **Tesla**, **ONStar**, and every GPS circuit in any car
- Smart pens (like the **Livescribe**)

- Gesture control devices (such as the **Leap**)
- SD cards
- Worlds of Warcraft and all online gaming networks like **Sony Network, Playstation Network, Nintendo Network**, etc.
- **ANY "Social Media**".
- ANY **online dating site**.
- Anything online that collects "**BIG DATA**" or any website that sends it's user information to a "Big data" service.
- Any website which asks you to photograph your location, particularly if it uses JPEG, or similar images, as **JPEG** has your location and personal data embedded in it.
- Any website which **asks you to write about yourself**, or your activities at any given moment, thus creating a psychological profile of you.
- Cameras
- Smart alarm clocks
- Anything that goes across **Amazon.com's** cloud servers as Amazon hosts the servers for spy agencies and hackers can easily get into Amazon cloud.
- Smart coffee makers
- Key fobs
- Light **switches**
- Moisture sensors
- Any **RSA Company** security technology. (NSA paid RSA $10M to put a "back-door" in everything they make.
- Toll Plaza **Fast Pass, Fastrak, etc.**
- Kitchen and pantry trackers (such as **Egg Minder)**
- Wearable health devices: health wristwatches, health headbands, health shoes, etc.
- Insurance driving monitors, such as **Progressive's Snapshot** device
- Traffic lights (MIRT transmitters can change lights to green in two to three seconds) highway signs that spell out text
- Anything with a **power cord**
- Anything you do on **Netflix** with your mouse or keyboard
- Anything with **batteries**
- **Google Maps**- Anything you look at, type in or zoom into.
- Any previous website you subscribe to can be "spoofed" by hackers. You think you are Twitter or Facebook or Salon.com but you are actually on a clone-site on the hackers servers and the hacker is watching everything you do.
- Any window that can **vibrate from the voices nearby**
- Any ceramic item that can vibrate from the voices nearby
- Any metal item that can vibrate from the voices nearby
- Heart pacemakers
- Any **bills you pay**, the addresses you pay them at, and the trends of the things you use, ie: cable tvm utilities including all credit card usage, amounts and locations where you purchased
- Most auto tires because tires have **RFID chips** embedded in the rubber
- **Security cameras** on buses
- **Match.com** and **OKCupid**
- Security cameras in stores & restaurants
- Security cameras on city vehicles
- **Walmart** hidden biometric shopper data acquisition devices
- **"Big Data"** output you generate when you use any device on a network
- Any implanted medical device
- Aircraft instruments
- Anything the hackers from the **Defcon Conference** decide they want to try to get into
- Any **filling** in your mouth with a special kind of ceramic vibration area
- More coming...

If you are worried about whether something can be hacked, or not, just type: "can XXX be hacked" into the top 5 search engines (You will get a different set of answers with each one)

The top safety tips: Unplug, remove batteries, change passwords weekly, use the longest password length allowed, tape over any camera lens on your PC/phone/tablet, be security conscious.

Don't worry, thousands of companies have been launched, and funded, in the last few months to fix these problems. Just be careful until the new products, and standards, arrive in late 2014.

http://www.youtube.com/watch?v=XDZwiclxdNA

----

http://www.youtube.com/watch?v=nlc9-v143tg

http://www.youtube.com/watch?v=kztvCH8ud8A

MATCH.com/OKCUPID.com CRISIS

The **creepiest Honey Trap** system is the one we heard about at ProPublica where the owners of **Match.com/OKCupid.com** are closely connected to certain **political "interests"**. A source claimed that they allow those interests to scan their database with **photo-comparison software**. If the dating profile picture you posted on Match.com or OkCupid is a match for a person the "interests" want to run a Honey Trap on, the "interests" send in a fake date person to try to get info from you, or get you in a compromising situation. Very often the hot blonde you think you are writing to is some hairy fat male political operative in New Jersey. Both sites already have **a number of legal actions** for fake profiles. If true, and you are controversial, I suppose you can't date anymore... bummer!

Ed- PP

(PS- GHT:)

To see what kind of people work at match.com and okcupid.com, here is a tweet from **THE PR DIRECTOR** for MATCH.COM and OKCUPID.COM:

JUSTINE_SACCO_MATCHCOM

----

60 Minutes busts Amazon.com as front for spying. That means Amazon may already be targeted by cyber criminals. Be careful.

http://www.youtube.com/watch?v=t8s7NMTQj_s

Movies about how spies use hacking:

'THE CONVERSATION,' 1974

It used to take a lot more effort for the government, or private eyes, to eavesdrop on private conversations. Fortunately cellphones have made it all much easier.

'NORTH BY NORTHWEST,' 1959

The ultimate Alfred Hitchcock spy drama, this Cold War classic races from New York to Chicago to Rapid City, S.D. And, suitably enough, the moment when Cary Grant is finally told by the mysterious government operative what is really going on is drowned out by an airplane engine. Eva Marie Saint remains one of the best-dressed supersecret agents ever.

'SALT,' 2010

Evelyn Salt, respected CIA agent, is suddenly accused of being a rogue agent planning to kill the president of Russia. It's impossible to know who's trustworthy in this action-packed spy thriller, which poses the question: Who is this Evelyn Salt, and whom is she working for?

'THE MANCHURIAN CANDIDATE,' 1962

One of Frank Sinatra's best performances, as an officer investigating the ultimate political mole. The film was withdrawn for years after the assassination of President Kennedy in 1963. It remains intriguing and chilling. The film was remade in 2004, but the original remains one of the standout spy movies of all time.

'NO WAY OUT,' 1987

Another Hackman vehicle, "No Way Out" tells the story of a deep-cover Soviet agent working at the Pentagon and the chase to unmask him. A combination whodunit and spy-action film, the story builds to a surprising conclusion that's sure to boost your paranoia about who's who.

'THE BOURNE IDENTITY,' 2002

Based on the best-selling book and starring Matt Damon as the confused, amnesia-stricken Jason Bourne, the movie takes viewers on an action-packed ride. Great chases, surprising plot twists and double-crosses abound in the film and its two sequels.

'THREE DAYS OF THE CONDOR,' 1975

Robert Redford plays Joe Turner, a bookish CIA researcher and analyst who comes back from lunch one day to find all his co-workers murdered. Turner must use all his research and tradecraft to evade those who killed his comrades while trying to figure out who is responsible. Also starring Faye Dunaway, the movie delves into the moral gray areas and questionable ethics of the spy business.

THE PRESIDENT'S ANALYST,' 1967

Satirical comedy is the genre of this movie about government using the telephone company to pry into the lives of private citizens. James Coburn stars as the psychoanalyst chosen by a government spy agency to act as the U.S. president's analyst. Coburn's character finds himself caught in a global web of intrigue as spy agencies around the world try to capture him and glean the secrets he's learned as the president's psychiatrist.

'MISSION: IMPOSSIBLE — GHOST PROTOCOL,' 2011

The fourth in the “Mission: Impossible” series sees Tom Cruise reprising his role as a secret agent working for the IMF — no, not that IMF, the other one: the Impossible Missions Force). The usual thrill ride of action sequences and double-crosses fills the screen throughout.

‘EAGLE EYE,’ 2008

Shia LaBeouf stars in this movie about Stanford dropout Jerry Shaw, who goes on the run after his identical twin brother is killed and a mysterious voice on the telephone advises him that the FBI is about to arrest him. Networked devices controlled remotely by the mysterious voice on the phone are sure to get your fears of Big Brother going.
----

https://www.youtube.com/watch?v=kztvCH8ud8A

http://avaxho.me/video/Format/documentary/discovery_channel_track_me_if_you_can.html

http://12160.info/video/track-me-if-you-can

(C) ACLU:

spy_ON_YOU

8 Things You Won't Believe Can Be Hacked | Cracked.com

Sep 7, 2011 ... If movies are to **be** believed, hackers are mostly kept busy kickflipping over the pentagon before sleeping in Mom's basement. But neither ...

www.cracked.com/ article_19412_8-things-you-wont-**be**lieve-**can**-**be**-**hacked**.html - View by Ixquick Proxy - Highlight

Baby Monitors Can Be Hacked, And So Can Everything Else ...

Aug 15, 2013 ... Hackable baby monitors reveal the vulnerability of everyday things.

www.popsci.com/technology/article/2013-08/baby-monitors-**can**-**be**-**hacked** - View by Ixquick Proxy - Highlight

Avi Rubin: All your devices can be hacked | Video on TED.com

Could someone hack your pacemaker? At TEDxMidAtlantic, Avi Rubin explains how hackers are compromising cars, smartphones and medical devices, and ...

www.ted.com/talks/avi_rubin_all_your_devices_**can**_**be**_**hacked**.html - View by Ixquick Proxy - Highlight

TEDx — Just what can we hack? Cars, drones, GPS? At TEDxAustin ...

Jul 30, 2013 ... After news broke that two security researchers, Chris Valasek and Charlie Miller, **hacked** into the systems of moving cars with just a laptop, ...

blog.tedx.com/ post/ 56888711934/ just-**what**-**can**-we-hack-cars-drones-gps-at - View by Ixquick Proxy - Highlight

How do I know if my computer has been hacked? - Computer Hope

Steps on how to determine if your computer has been **hacked** by a hacker.

www.computerhope.com/issues/ch001296.htm - View by Ixquick Proxy - Highlight

Facebook hacked: how criminals can exploit your data - Telegraph

Oct 16, 2013 ... Information kept on Facebook could help fraudsters create credit cards, bank loans and new accounts in your name.

www.telegraph.co.uk/ technology/ facebook/ 10369934/ Facebook-**hacked**-how-criminals-**can**-exploit-your-data.html - View by Ixquick Proxy - Highlight

How to Hack: 12 Steps - wikiHow

Attempt to hack it in any way you **can**. Don't change the site, just make it yours. 3. Test the target. **Can** you reach the remote system? While you **can** use the ping ...

www.wikihow.com/Hack - View by Ixquick Proxy - Highlight

Rumor: Smartphones can hack into high-tech homes - News

Aug 13, 2013 ... **Can** your high-tech "smart home" — including your door locks — **be hacked** into and taken control of by someone on the other side of the ...

news.msn.com/rumors/rumor-smartphones-**can**-hack-into-high-tech-homes - View by Ixquick Proxy - Highlight

Can Your Car Be Hacked? - Feature - Car and Driver

Protecting your car used to involve making sure it was locked, and maybe even a Club affixed to the steering wheel, but in the not-so-distant future, cars will ...

www.caranddriver.com/features/**can**-your-car-**be**-**hacked**-feature - View by Ixquick Proxy - Highlight

http://www.youtube.com/watch?v=i3S0XAmLmrM

How Easily Can a Moving Car Be Hacked? | Motherboard

With the conspiracy theory that Michael Hastings' car was **hacked** swirling about, we look into auto-hacking.

motherboard.vice.com/blog/how-easily-**can**-a-moving-car-**be**-**hacked** - View by Ixquick Proxy - Highlight

Hack This Site!

Hack This Site is a free, safe and legal training ground for hackers to test and ... of hacking articles and a huge forum where users **can** discuss hacking, network ...

www.hackthissite.org - View by Ixquick Proxy - Highlight

Your Twitter account has been hacked! Here's what to do about it ...

Sep 9, 2013 ... Kirsty woke up to find that someone else had taken control of her account. I tell her how to get it back.

www.pcworld.com/ article/ 2047286/ your-twitter-account-has-**be**en-**hacked**-heres-**what**-to-do-about-it-.html - View by Ixquick Proxy - Highlight

I think someone has hacked my account, what can I do? - Help

Let us know the account permalink and email address that you set up your account with and we **can** take a look at **what**'s going on. If this account hacking is ...

help.soundcloud.com/ customer/ portal/ articles/ 367394-i-think-someone-has-**hacked**-my-account-**what**-**can**-i-do- - View by Ixquick Proxy - Highlight

Cyber-Attack in the Bathroom: Japanese Toilet Can Be Hacked | The ...

Aug 5, 2013 ... Bluetooth vulnerability allows one brand of Japanese toilet to **be** operated remotely.

www.thediplomat.com/ 2013/ 08/ cy**be**r-attack-in-the-bathroom-japanese-toilet-**can**-**be**-**hacked**/ - View by Ixquick Proxy - Highlight

Top 9 Things To Do After Your Email is Hacked - ABC News

Jul 21, 2013 ... For many people, the first sign that their email has been **hacked** comes when a friend shoots them a text or an email saying, "Hey there. Uh… I ...

abcnews.go.com/Business/top-things-email-**hacked**/story?id=19715483 - View by Ixquick Proxy - Highlight

CAN Hacking: Introductions - Hack a Day

Oct 21, 2013 ... We're introducing a new series on **CAN** and automotive hacking. First, we'll introduce **CAN** and discuss how in-vehicle networks work. In 1986 ...

www.hackaday.com/2013/10/21/**can**-hacking-introductions/ - View by Ixquick Proxy - Highlight

Your Car Can Be Hacked And Here's What It Might Look Like: Video

Jul 29, 2013 ... A team of computer security experts aims to explain exactly **what can be** accomplished when it comes to hacking a car. Modern vehicles are ...

www.motorauthority.com/ news/ 1085863_your-car-**can-be-hacked**-and-heres-**what**-it-might-look-like-vide o - View by Ixquick Proxy - Highlight

Don't Think Your Car Can Be Hacked? Watch This Terrifying Video ...

Jul 26, 2013 ... If you're at all the slightest bit skeptical of the emerging capability of hackers to take control of your electronic devices, then don't watch this ...

www.theblaze.com/ stories/ 2013/ 07/ 26/ the-terrifying-5-minute-video-showing-how-its-possible-to-hack-a-car- and-make-it-do-some-freaky-things/ - View by Ixquick Proxy - Highlight

IPhones can be hacked while charging - USA Today

Nov 12, 2013 ... ATLANTA — You'll want to read this story. Your security could depend on it. The popular iPhone has won praise over its resistance to hackers ...

www.usatoday.com/ story/ tech/ personal/ 2013/ 11/ 12/ iphone-hack-while-charging/ 3505753/ - View by Ixquick Proxy - Highlight

I think somebody has hacked my Origin Account. What can I ... - Help

Sep 20, 2013 ... The following process should **be** followed if you believe that your Origin (EA) Account has been **hacked** or compromised. If you have been ...

https://help.ea.com/ article/ i-think-somebody-**hacked**-my-origin-account-**what**-**can**-i-do-now - View by Ixquick Proxy - Highlight

Can your "smart TV" watch you? - CBS News

At a demonstration Friday in Las Vegas, researchers showed an audience of children at Defcon Kids how a Samsung Smart TV **can be hacked**. So-called smart ...

www.cbsnews.com/news/**can**-your-smart-tv-watch-you/ - View by Ixquick Proxy - Highlight

Your Smart TV Could Be Hacked to Spy On You - Mashable

Aug 2, 2013 ... As in turns out, just like smartphones, Smart TVs **can be hacked** and compromised. On Thursday, at the Black Hat security conference, ...

www.mashable.com/2013/08/02/samsung-smart-tv-hack/ - View by Ixquick Proxy - Highlight

Twitter Help Center | My account has been compromised

Unexpected updates don't always mean that your account was **hacked**. Occasionally, a third-party application **can** have a bug that causes unexpected behavior.

https://support.twitter.com/ articles/ 31796-my-account-has-**be**en-compromised - View by Ixquick Proxy - Highlight

So Dropbox Can Be Hacked—What Else Is New? – ReadWrite

Aug 28, 2013 ... Researchers reverse engineer the cloud storage service to bypass two-factor logins and hijack accounts. Big deal.

www.readwrite.com/2013/08/28/dropbox-**hacked**-reverse-engineered-client - View by Ixquick Proxy - Highlight

iPhone 5S fingerprint sensor hacked by Germany's Chaos Computer ...

Sep 23, 2013 ... In a post on their site, the group says that their biometric hacking team ... Another found that the Emergency Call screen **can be** used to place a ...

www.theguardian.com/ technology/ 2013/ sep/ 22/ apple-iphone-fingerprint-s**can**ner-**hacked** - View by Ixquick Proxy - Highlight

I have had my account hacked and my profile altered. What can I do ...

The issue is no response from the Safety and Trust Team in 10 days. My profile was **hacked** on the 20th June, (despite a strong password with letters, numbers ...

community.linkedin.com/ questions/ 35874/ i-have-had-my-account-**hacked**-and-my-profile-altere.html - View by Ixquick Proxy - Highlight

Twitter Help Center | My account has been hacked

If you still **can**'t log in, contact us by submitting a Support request. Please choose "**Hacked** account" from the list of options. **Be** sure to use the email address you ...

https://support.twitter.com/ articles/ 185703-my-account-has-**be**en-**hacked** - View by Ixquick Proxy - Highlight

Hacked Accounts | Facebook Help Center | Facebook

Hacked Accounts. My Account. My account is **hacked**. If your ... My account was **hacked** and used to make purchases on apps and/or with Facebook credits.

https://www.facebook.com/help/www/131719720300233 - View by Ixquick Proxy - Highlight

Someone hacked my AOL Mail account. What do I do? - AOL Help

Oct 18, 2013 ... 1. Go to account.aol.com immediately and change your password. Use a mix of upper & lowercase letters, numbers, and special characters in ...

help.aol.com/ article/ someone-**hacked**-my-aol-mail-account-**what**-do-i-do--/ 86577 - View by Ixquick Proxy - Highlight

If Apple's iPhone Has Fingerprint Authentication, Can It Be Hacked ...

Sep 9, 2013 ... Apple would **be** smart to add biometric technology to the iPhone. Fingerprint authentication is a good balance between convenience and ...

www.wired.com/ opinion/ 2013/ 09/ **what**-if-apples-new-phone-has-fingerprint-authentication/ - View by Ixquick Proxy - Highlight

----

Option #6: "The Hack and Block"- (see more at THIS LINK)

Did you ever think you were doing everything right and things inexplicably go south right at the last minute? If you are a reporter or a public service person, you might be under the watch of a Hack and Block Operative. These technical hackers are already inside your phone and computer via embedded backdoors and spyware. Most of the time they do not even have to watch as you type. They just program their spyware to look for a selection of keywords that may have something to do with what they want to block. For example, if you are working on a story about stuffed animals and toxins, they might program their spyware to resend them anything with the words: "teddy bear, mattel, stuffed, stuffing, elmo, toys, investigation...etc" and on and on for thousands of words. The second you type one of these things, the political operative gets a text about it and goes to work. Did you just set up a meeting with an investor? That investor suddenly gets an anonymous tip with damaging info about you and the meeting is "rain-checked".. Did you just set up a date online? Your date gets a disturbing message about you and suddenly she is "busy". Did you just try to source a great tip for an interview? Suddenly the tip source "wants to think about it some more"? Your Operative got mail and you got Blocked.

Also known as "Hack-And-Extort"!

Ideal counter measures are: Massive disinformation output, never keep anything connected to any network (ie: unplug all power cords and network cables), only write fake meeting dates in electronic calendars, encrypt, relay, tor, create false lead traps that end up at your litigation firm's office, put black electrical over every camera lens, phone lens, tablet lens, webcam lens, smart tv lens, computer lens, etc.

One of the more **horrific** uses of **Hack and Block** is this story, an act which **every American is now at risk of** if you don't **put black electrical tape over every camera lens** on your phone, tablet and computers:

LIBERTY-VOICE

http://guardianlv.com/2013/12/apple-inc-and-other-webcams-hacked-miss-teen-usa-nude-photos-taken/

Apple Inc. And Other Webcams Hacked – Miss Teen USA Nude Photos Taken

Added by Brent Matsalla on December 21, 2013.
Saved under Apple, Brent Matsalla, Technology
Tags: apple inc, top

http://guardianlv.com/wp-content/uploads/2013/12/Apple-Inc.-And-Other-Webcams-Hacked-Miss-Teen-USA-Nude-Photos-Taken-650x361.jpg

Researchers at the Department of Computer Science at Johns Hopkins University say that Apple Inc.'s iSight camera system among other webcams can be vulnerable to hijack hacking. However, 19-year-old Miss Teen USA, Cassidy Wolf, found out the hard way when she received an anonymous email containing two nude photos of herself that were taken by her own hacked webcam.

The email demanded more nude photos from Wolf or the anonymous sender threatened to release her photos to the public if she didn't comply. More demands were also made in the email, but the details of these demands were not shared.

http://guardianlv.com/wp-content/uploads/2013/12/Apple-Inc.-And-Other-Webcams-Hacked-Miss-Teen-USA-Nude-Photos-Taken2-450x382.jpg

The nude photos were taken over several months by Wolf's own laptop webcam. Wolf said that her webcam light never came on during this period, which would have tipped her off that her webcam was in use. It was never confirmed whether the webcam light had been disabled by the hacker, or if Wolf just didn't realize the LED light being on. ***The hacker was spying on her and through up to 150 other webcams in the area.***

The FBI says suspected hacker, Jared Abrahams, breached the privacy of people by hacking into their webcams with his sophisticated network and peeping software. Abrahams has now pled guilty to extortion charges.

Earlier this month the FBI also revealed that they have been using a malicious software program called “malware” as a spying technique on suspects through the suspect’s own webcams. The malware program was able to allow surveillance without toggling on the “in-operation” LED light located on a suspect’s webcam. This is a similar sounding observation described by Miss Teen USA when her webcam was hacked and the nude photos were taken. Apple Inc.’s and other webcams have a hardware interlock between the LED light and the webcam. When the webcam is in operation, the LED light is always supposed to be toggled to the on position automatically.

Assistant professor and co-author of the Johns Hopkins’ paper – *iSeeYou,* Stephen Checkoway, says that he and his partner were able to hack into Apple Inc.’s iSight camera system and disable the LED light when the camera was operating. Checkoway and his paper’s co-author, Matthew Brocker, were able to independently control the camera to record audio, video, and snap pictures without enabling the camera’s integrated LED light. The team was able to accomplish their feat by reprogramming the microcontroller contained within the iSight camera system.

Checkoway and Brocker notified Apple Inc. about their ability to exploit the iSight camera system, and although Apple did not reply to requested comments, Apple sources say they took this very serious. The researchers did follow up with Apple several times, but were not informed by any possible plans for mitigation. Checkoway did note that the exploit now only works on older 2008 Apple products.

The federal government made agreements with seven computer rental companies last year, when it was discovered that they were unlawfully spying on their customers. The companies were allegedly capturing photos of their customers through the rental computer’s webcam.

Miss Teen USA is only one case where nude photos have been taken from a hacked webcam. Apple Inc. and other webcam manufacturers will always remain vulnerable to malware hacking programs. The Federal Trade Commission says that currently many thousands of people may be getting spied on from webcam software named PC Rental Agent. This program had previously been installed on approximately 420,000 computers across the world. When it’s not in use, covering the webcam with a piece of paper remains to be the best security from any hacked webcam.

By Brent Matsalla

Sources:
New York Times
Techland
Washington Post

(PS: GHI- A number of auto execs/agency heads have quit, or are sleeping in fear, because they believe they got Hack & Blocked doing bribery, WITH VIDEO, and their numbers may be about to come up in federal investigations. I'd say keep on eye out for Mother Jones or ProPublica's next video undercover exclusive from the tipsters ;-) ......)

EU Asks Advertisers: Does Google Manipulate Its Search Results ...

Jan 13, 2011 ... Hey, advertisers in the European Union. **Does Google** give you better organic **results** if you spend more in AdWords, or have they promised you ...

www.searchenginewatch.com/ article/ 2050178/ EU-Asks-Advertisers-**Does**-**Google**-**Manipulate**-**Its**-Search-**Results** - View by Ixquick Proxy - Highlight

Is Google's search manipulation hurting consumer? | Digital Trends

Nov 25, 2012 ... **Google** Shopping search **results** manipulation. Way back in 1998 when **Google** launched, **its** core product was search and **its** main customer ...

www.digitaltrends.com/web/bias-and-**google**-shopping/ - View by Ixquick Proxy - Highlight

Facts about Google and Competition

Does Google ever penalize **its** competitors in **its** search **results**? Do quality scores allow **Google** to **manipulate its** ad auction? Can **Google**'s advertisers export ...

https://www.**google**.com/competition/qa.html - View by Ixquick Proxy - Highlight

Google's Secret Search Algorithm Could Manipulate the Results of ...

Jun 16, 2013 ... A study indicated that manipulating **Google results** could influence ... Looking into **its** fibrous nexus is like looking into a mirror, one which is ...

www.policymic.com/ articles/ 49035/ **google**-s-secret-search-algorithm-could-**manipulate**-the-**results**-of-an-e lection - View by Ixquick Proxy - Highlight

Google Allegedly Manipulating Search Results Favoring Big Brands ...

Oct 15, 2012 ... So for **Google** to claim there were “quality issues” with his site is like ... they were accused of using **Google** Instant to **manipulate** search **results**, ...

www.infowars.com/ **google**-allegedly-manipulating-search-**results**-favoring-big-brands-over -small-businesses/ - View by Ixquick Proxy - Highlight

Does Google manipulate search results for it's own gain? - Las ...

Sep 21, 2011 ... In a congressional hearing that is taking place today, The Federal Trade Comission is looking into the charge that **Google** Inc manipulates it's ...

www.examiner.com/ article/ **does-google-manipulate**-search-**results**-for-it-s-own-gain - View by Ixquick Proxy - Highlight

Competitor Sues Company For Manipulating Google's Search Results

Feb 11, 2013 ... Legally Accused Of Manipulating **Google**'s Search **Results** ... a competitor for manipulating the search **results** to make their competitor look bad in **Google**. This company is seeking an "SEO expert" to write a legal letter to help ...

www.seroundtable.com/legal-manipulating-**google**-search-16342.html - View by Ixquick Proxy - Highlight

Criticism of Google - Wikipedia, the free encyclopedia

The page ranking algorithm of **Google** can and has been ... **Google** rigs **its results** , biasing in favor of **Google** ...

https://en.wikipedia.org/wiki/Criticism_of_**Google** - View by Ixquick Proxy - Highlight

Google bomb - Wikipedia, the free encyclopedia

In the article Mathes details his connection of the search term "talentless hack" to the .... As of May 2, 2011, the page is no longer listed in **Google**'s first few **results** for "French military .... "A New Campaign Tactic: Manipulating **Google** Data".

https://en.wikipedia.org/wiki/**Google**_bomb - View by Ixquick Proxy - Highlight

Does Google Manipulate Search Placement at the Expense of ...

Sep 13, 2011 ... This is an admission by **Google** of how it used **its** search dominance to ... Typically, the top ranked result gets three-and-a-half times as many ...

www.actonline.org/act-blog/archives/1872 - View by Ixquick Proxy - Highlight

Google's Search Manipulation Opens SEO Opportunity - Jon ...

Jan 13, 2012 ... Whether **Google**'s manipulation of search **results** to prioritize **Google**+ content is ethical or not, it's an SEO opportunity for publishers.

www.jonloomer.com/ 2012/ 01/ 13/ **google**s-search-manipulation-opens-seo-opportunity/ - View by Ixquick Proxy - Highlight

The Security Risks of Unregulated Google Search - Schneier on ...

Jun 4, 2013 ... Could **Google** tip an election by manipulating what comes up from search ... Conservatives will get **results** favoring conservative candidates, liberals get .... It's well established that search **results** have monetary value: see both ...

www.schneier.com/blog/archives/2013/06/the_security_ri_3.html - View by Ixquick Proxy - Highlight

----

SALON ANDREW_LEONARD How to defeat Big Brother

In 2013, we learned the terrifying scope of modern surveillance. Now it's time to fight back

Andrew Leonard

“Visibility is a trap.”

It can be safely argued that those four words, written by the French philosopher Michel Foucault in his discussion of the “panopticon,” were never more true than they were this year. Our visibility — defined as ubiquitous, networked digital connectedness — has at long last enabled an unprecedented surveillance state. In 2013, the negative consequences of our contemporary lifestyles were impossible to ignore.

But not just for the most obvious reason — the avalanche of revelations about the depth and scope of government spying delivered by Edward Snowden, which seized the world's attention from June onward. The surveillance society is hardly limited to NSA spooks. We are now open books for *everyone* to read: Our friends and our enemies and our stalkers. Our providers of email and texting and social media and advertising and entertainment. Our employers, our doctors and our teachers. We have never been more visible, never been more willing or able to open up every moment of our existence to the outside world. And in doing so, we have handed the watchers fantastic power.

When you use something as seemingly innocuous as the flashlight app on your smartphone, it's entirely possible that your location data is being gathered. The particular constellation of apps you use most often is exploited to build a profile for targeted advertising. Netflix makes note of every time you pause or fast-forward an episode of "Orange is the New Black." Facebook is analyzing even the status updates that you delete before posting. Google Now knows when and where I am traveling, what packages are on the way to my house, and, of course, what I have been searching for recently. Your employer is gathering every conceivable data metric for evaluating your job performance.

Visibility is a trap. The convenience of the smartphone is a trap. The web of connectivity that binds us into a seething, ADHD hive mind is a trap. Our daily lives are constructed out of ones and zeroes and because they *can* be counted, they *will* be counted.

But understanding this fact is, and must be, the first step toward escape; the Panopticon doesn't work if we watch the watchers back. Knowing exactly how we are being surveilled is the set-up for a prison break.

* * *

In its original formulation by the 18th century philosopher Jeremy Bentham, the "Panopticon" was an instrument of control, "a new mode of obtaining power of mind over mind, in a quantity hitherto without example."

The Panopticon, in Bentham's formulation, is a building in which a single watchman or "inspector" can see every prisoner "without being seen" himself. The theory is that if we know it is *possible* that someone is watching us, we will behave ourselves accordingly, even if no one is actually minding the store. The concept, as imagined by Bentham, applied to much more than just your local jail.

> No matter how different, or even opposite the purpose: whether it be that of punishing the incorrigible, guarding the insane, reforming the vicious, confining the suspected, employing the idle, maintaining the helpless, curing the sick, instructing the willing in any branch of industry, or training the rising race in the path of education: in a word, whether it be applied to the purposes of perpetual prisons in the room of death, or prisons for confinement before trial, or penitentiary-houses, or houses of correction, or work-houses, or manufactories, or mad-houses, or hospitals, or schools.

At first glance, our ubiquitous closed circuit camera society — in which every keystroke might be logged, and the FBI could be watching us through our laptop camera, our GPS-enabled tablets and phones have become "NSA primate-tracking devices," and the content of our emails is being analyzed by Google's algorithms — maps quite nicely to the all-purpose utilitarianism of the Panopticon. We are all constantly being inspected; or, in what amounts to the same thing, we all *might* be under constant inspection.

> It is obvious that, in all these instances, the more constantly the persons to be inspected are under the eyes of the persons who should inspect them, the more perfectly will the purpose X of the establishment have been attained. Ideal perfection, if that were the object, would require that each person should actually be in that predicament, during every instant of time. This being impossible, the next thing to be wished for is, that, at every instant, seeing reason to believe as much, and not being able to satisfy himself to the contrary, he should conceive himself to be so.

The irony here is that what Bentham conceived of as impossible — all the people in any given institution being watched, "during every instant of time" — is now quite within the realm of possibility, if we count the artificially intelligent algorithms chewing away at all our "big data" as essentially the same thing as Bentham's all-seeing inspector. Certainly, no single human can read all our emails or texts, listen in to all our phone calls, track all our movements or record every song we listen to on our Sonos wireless systems or every TV show we watch on Netflix. The sheer volume of data that we are producing far outstrips the cognitive capacity of the mere human mind.

But the same networked computers that give us so much amazing access to everything that humans have ever written (or composed, or photographed) have unhappily returned the favor by making it possible to sift through that infinite firehose of data. The inspector is now everywhere — and again, at first glance, that appears to satisfy the conditions postulated by Bentham. I don't *know*whether the FBI or NSA is watching me type these words through my laptop camera or keylogging software, but they could be, right? So I'd better watch out, right? I'd better be good?

Maybe.

What, ultimately, does it mean for us to know that everyone from the NSA to our boss to Netflix to Google could be tracking us and number-crunching us and targeting us? Does it mean we behave any differently, as Bentham predicted? Are we better consumers, buying what we're supposed to buy? (Probably.) Are we more passive citizens, refraining from activism or dissent? (Almost certainly not.) Are we more diligent and productive workers?

It's probably too early to make any conclusions from the data that has been gathered so far. We're engaged in a huge, open-ended laboratory experiment with no control group to compare ourselves to. The science of "people analytics" is still in its infancy.

But one of the great paradoxes of the digital era is that even though we know we have no privacy, it doesn't seem like very many people act accordingly. We embarrass ourselves on social media all the time. We construct track records for our employers and governments to pore over with hardly a second thought. There are some signs that we are beginning to seek out more privacy-conscious modes of living (See: Snapchat) but in general, we seem perfectly willing to live our lives in full-frontal public view. Tamerlan Tsarnaev's Amazon wish list included five books on forging documents and making fake IDs!

So Bentham's primary justification of the Panopticon — the notion that the illusion that someone is watching will encourage the proper behavior intended by whatever institution employs the technique — doesn't appear to be borne out by contemporary practice. Furthermore, Bentham's Panopticon only worked in one direction, whereas our surveillance-enabling devices also give us great individual power. One second after the first person posts on Facebook that the FBI might be able to spy through our laptop computers, the entire world has shared this information. Forewarned is forearmed, right?

If we know that advertisers are watching our iPhone apps to figure out what kind of customer we are and what we are most likely to buy, shouldn't that give us some agency in the equation? Shouldn't that knowledge — that what's been presented to us is no accident — engender skepticism and wariness?

If 2013 was the year in which we finally started to grasp the awesome scope of the surveillance — that our daily lives are exposed to all the watchers out there, all the time and by multiple inspectors — then maybe 2013 is also the year in which we started to figure out what the truly appropriate response to our predicament should be.

Here's hoping it's not what the operators of these panopticons are hoping for. Let's make some noise in 2014!

Edward Snowden, whether one considers him a traitor or a hero, indisputably put the issue of government spying on the national table, and provoked a conversation that seems likely to have real political consequences. He used the technology available to him to turn the camera back on the watchers. It's a model we should be following in every domain. Let's turn a closer eye on our employers and our content providers and our advertisers.

Maybe the full potential of the Panopticon will only be realized when everybody — the powerless and the powerful, the leaders and the led, the stalkers and the stalked — realizes that everyone is watching everything. Maybe then, we'll be able to achieve a respectable state of civilization. Maybe then, the "trap" of "visibility" will turn out to liberate, rather than imprison.

BILLBOARDS

The Most Whack Use of Hacking: Hacking Your Brain Via the Internet!

Ready for the ultimate extreme hack? We mean, **wayyyy over the top**. ...and this is the "old Technology", imagine what the modern versions can do. Las Vegas already has companies testing things like this to increase gambling, big Malls use entry-level versions of these technologies to increase sales:

Exposed: The Soviet Union spent $1 billion on mind-control program

Dr. Bill van Bise, electrical engineer, conducting a demonstration of Soviet scientific data and schematics for beaming a magnetic field into the brain to cause visual hallucinations. Source: CNN *Source:* Supplied

THE race to put man on the Moon wasn't enough of a battle for the global super powers during the Cold War.

At the time, the Soviet Union and the United States were in an arms race of a bizarre, unconventional kind - that has been exposed in a new report.

Beginning in 1917 and continuing until 2003, the Soviets poured up to $1 billion into developing mind-controlling weaponry to compete with similar programs undertaken in the US.

While much still remains classified, we can now confirm the Soviets used methods to manipulate test subjects' brains.

The paper, by Serge Kernbach, at the Research Centre of Advanced Robotics and Environmental Science in Stuttgart, Germany, details the Soviet Union's extensive experiments, called "psychotronics". The paper is based on Russian technical journals and recently declassified documents.

Still from<i> Secret Russia: Moscow The Zombies of the Red Czar</i>, a German TV...

Still from *Secret Russia: MoscowThe Zombies of the Red Czar*, a German TV documentary, 1998. *Source:* Supplied

The paper outlines how the Soviets developed "cerpan", a device to generate and store high-frequency electromagnetic radiation and the use of this energy to affect other objects.

"If the generator is designed properly, it is able to accumulate bioenergy from all living things - animals, plants, humans - and then release it outside," the paper said.

The psychotronics program, known in the US as "parapsychology", involves unconventional research into mind control and remote influence - and was funded by the government.

With only limited knowledge of each other's mind-bending programs, the Soviets and Americans were both participating in similar secret operations, with areas of interest often mirroring the other country's study.

The original scheme of transmitting and receiving bio-circuitry of the human nervous system. Picture: B. B. Kazhinskiy *Source:* Supplied

(NOTE: GHH- The Movie: **The Matrix**, proposed that humans would become batteries for the robots. The soviet "Cerpan" system seems to already be doing that, per this study.)

The psychotronics project draws similarities to part of the controversial program MKUltra in the US. The CIA program ran for 20 years, has been highly documented since being investigated in the 1970s and was recently dramatised in the movie *The Men Who Stare at Goats.*

The Men Who Stare at Goats. Picture: Smokehouse Pictures

The Men Who Stare at Goats. George Clooney. Picture: Smokehouse Pictures *Source:* Supplied

Scientists involved in the MKUltra program researched the possibility of manipulating people's minds by altering their brain functions using electromagnetic waves. This program led to the development of pyschotronic weapons, which were intended to be used to perform these mind-shifting functions.

The illegal research subjected humans to experiments with drugs, such as LSD, hypnosis and radiological and biological agents. Shockingly, some studies were conducted without the subject's knowledge.

A US Marine Corps truck carries an Active Denial System. It is a nonlethal weapon that uses directed energy and projects a beam of waves up to 1000 metres. When fired at a human, it delivers a heat sensation to the skin and generally makes humans stop what they are doing and run. *Source:* AAP

Kernbach's paper on the Soviet Union's psychotronics program fails to mention one thing - the results. He also doesn't detail whether there are ongoing programs in this area in the US or Russia, which became the successor state of the Russian SFSR following the dissolution of the Soviet Union in 1991, but there are suspicions.

Putin made mention of futuristic weaponry last year in a presidential campaign article.

"Space-based systems and IT tools, especially in cyberspace, will play a great, if not decisive role in armed conflicts. In a more remote future, weapon systems that use different physical principles will be created (beam, geophysical, wave, genetic, psychophysical and other types of weapons). All this will provide fundamentally new instruments for achieving political and strategic goals in addition to nuclear weapons," he wrote.

Example of a generator from the psychotronics program.

Example of a generator from the psychotronics program. *Source:* Supplied

The newly declassified information outlined in the report only touches on the Soviet psychotronics program and the bizarre experiments undertaken. With so much information still classified, will we ever know the whole truth?

Continue the conversation on Twitter @jennijenni | @newscomauHQ

Unconventional research in USSR and Russia- By Arkadiusz Jadczyk via Sott.net Sun, 22 Dec 2013

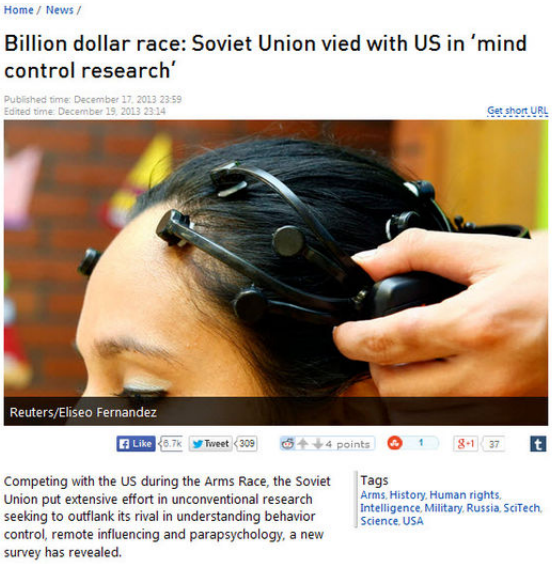
- Posted by UnitedWeStand on December 26, 2013 at 12:07pm
- View Blog

Unconventional research in USSR and Russia -- Science & Technol...

Arkadiusz Jadczyk Sott.net Sun, 22 Dec 2013

Summary: Unconventional research embraces physics, artificial intelligence and the paranormal.

Cf. 'Billion dollar race: Soviet Union vied with US in 'mind control research'', Russia Today, December 17th, 2013



Home / News /

Billion dollar race: Soviet Union vied with US in 'mind control research'

Published time: December 17, 2013 23:59
Edited time: December 19, 2013 23:14

Get short URL

Reuters/Eliseo Fernandez

Competing with the US during the Arms Race, the Soviet Union put extensive effort in unconventional research seeking to outflank its rival in understanding behavior control, remote influencing and parapsychology, a new survey has revealed.

Tags
Arms, History, Human rights, Intelligence, Military, Russia, SciTech, Science, USA

The title of this article comes from a recent paper by Serge Kernbach:

'Unconventional research in USSR and Russia: short overview', Serge Kernbach (Submitted on 4 Dec 2013 (v1), last revised 5 Dec 2013 (this version, v2))

> This work briefly surveys unconventional research in Russia from the end of the 19th until the beginning of the 21th centuries in areas related to generation and detection of a 'high-penetrating' emission of non-biological origin. The overview is based on open scientific and journalistic materials. The unique character of this research and its history, originating from governmental programs of the USSR, is shown. Relations to modern studies on biological effects of weak electromagnetic emission, several areas of bioinformatics and theories of physical vacuum are discussed.

Nowadays almost every physicist is monitoring, one way or another, all the new papers in her/his domain of interest. The arxiv site is probably the most popular one among physicists, mathematicians and computer science researchers. It is not completely easy to submit a paper there. Not that there is a peer-review process there, but some kind of endorsement from some "well-established" scientist is needed. Otherwise your paper will not be accepted for pre-publication. Why was Kernbach's paper accepted? Because he has 16 papers already there. And also, probably, because of his affiliation:

Cybertronica Research, Research Center of Advanced Robotics
and Environmental Science, Melunerstr. 40, 70569 Stuttgart, Germany

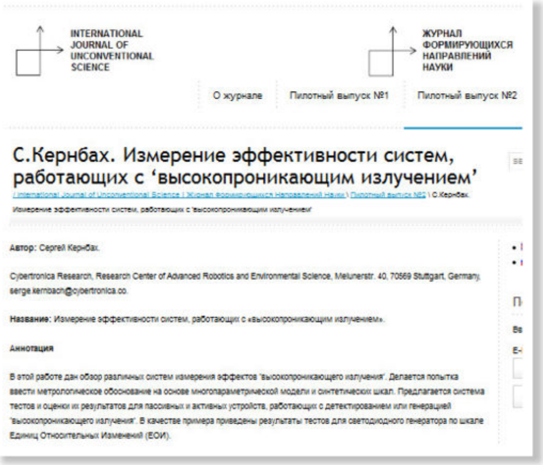
Checking the publications of Serge Kernbach we find that his main interest is in the science and practice of robotics, mainly in "swarms of robots". An army of mini-robots can today be programmed to act in a way similar to the behavior of ants and/or bees. Look at these videos - they are amazing, and also somewhat scary:

But why does an expert in swarms of robots get interested in "unconventional research" that has to do with physics?

This question came to my mind after his paper caught my attention. So I started a little research of my own. The article has also the comment stating that:

> 2) V.1.4. Russian version of this work is submitted to the*International Journal of Unconventional Science*

So I checked what it is that Serge Kernbach is publishing in Russian rather than in English? Well, it appears that he is one of the co-founders of the *Journal of Unconventional Science*. In the first issue of this online journal there is an introductory article, written together with Vlad Zhigalov, in which the Editors touch the subjects of scientific ethics, and also describe the way the new journal will work. Then there is another paper, also written with Vlad Zhigalov, in which they describe a series of experiments on the "phantom effect" - one of the effects that are sometimes classified as belonging to "the paranormal". But even more interesting is Kernbach's paper in the most recent issue of the *Journal*:



INTERNATIONAL JOURNAL OF UNCONVENTIONAL SCIENCE

ЖУРНАЛ ФОРМИРУЮЩИХСЯ НАПРАВЛЕНИЙ НАУКИ

С.Кернбах. Измерение эффективности систем, работающих с 'высокопроникающим излучением'

/ International Journal of Unconventional Science | Журнал формирующихся Направлений Науки \ Пилотный выпуск №2 \ С.Кернбах. Измерение эффективности систем, работающих с 'высокопроникающим излучением'

Автор: Сергей Кернбах.

Cybertronica Research, Research Center of Advanced Robotics and Environmental Science, Melunerstr. 40, 70569 Stuttgart, Germany, serge.kernbach@cybertronica.co.

Название: Измерение эффективности систем, работающих с «высокопроникающим излучением».

Аннотация

В этой работе дан обзор различных систем измерения эффектов 'высокопроникающего излучения'. Делается попытка ввести метрологическое обоснование на основе многопараметрической модели и синтетических шкал. Предлагается система тестов и оценки их результатов для пассивных и активных устройств, работающих с детектированием или генерацией 'высокопроникающего излучения'. В качестве примера приведены результаты тестов для светодиодного генератора по шкале Единиц Относительных Изменений (ЕОИ).

It follows from this article that Kernbach is interested in "highly penetrating radiation". In fact he is an inventor of some of the devices that produce such a "radiation". The physical nature of this radiation is not clear. It may act both on physical devices and on biological systems as well. It can penetrate walls and act at a distance, even 'faster than light".

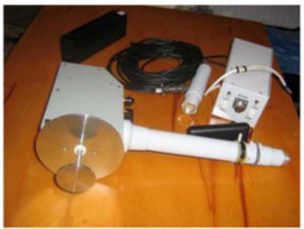


Рис. 117. Индикатор геофизических аномалий - ИГА-1.

© www.second-physics.ru

One of the commercially available detectors of the "higly penetrating emission" - IGA1. From a paper by V. Zhigalov "Harakternye jeffekty nejelektromagnitnogo izluchenija" 2011

Yet, until now, it belongs to the "fringe science", "pseudo-science" or "false science". In fact, sometimes publications dealing with this subject find their way to the mainstream physics journals, but always under disguise.

We can ask now again: why is it that Serge Kernbach, an expert in artificial intelligence and swarms of robots, is also interested in "paranormal phenomena" (or in "psychotronics", as it was called in Russia)?

A partial answer to this question may be guessed from the referee report published under the article in *The International Journal of Unconventional Science*. The report is written by **A. Yu. Smirnov**, another expert in "radiation of unknown nature", and inventor of another "generator" of such a radiation.

Smirnov discusses there the role of "information" and the role of the "human operator" in experiments with similar devices, both generators and the detectors. These subjects appear to be neglected in the article by Kernbach. Smirnov suggests that one reason for these omissions and for the fact that Kernbach is mainly interested in some kind of an official "certification" of similar devices, may be the commercial reason. It would be nice if we can equip robots with similar sensors, let them communicate using not-well-understood but sometimes very effective processes, and sell them. Here are just two sentences from Smirnov's review:

> *Таким образом, можно предположить, что у автора речь идет, не больше и не меньше - о сертификации генераторов и приемников ВИ, по-видимому, как необходимого этапа к подготовке к массовому, в том числе, коммерческому использованию приборов: генераторов, а, возможно, и детекторов "высокопроникающего излучения".*
>
> *Это нормальная, понятная позиция, но только причем здесь наука?*

In translation:

> *This way, we can assume that what the author has in mind is just that: certification of generators and detectors of "highly penetrating radiation", evidently as a necessary step for mass production, including the commercial use of the devices: generators and, perhaps, also detectors of the "highly penetrating radiation".*

> *Such an approach is understandable, but what has it* to do with science?

The original article by Serge Kernbach, the one about "Unconventional research in USSR and Russia", the one that was featured on Russia Today, tells us about the research up until 2003. What happened after that? Well, after that Serge Kernbach himself is busy with his own unconventional research.

As the subject touches several areas of physics that are within my own domain of scientific interest, I am going to write more about these subjects in forthcoming articles.
Update: After posting this article I have received the following additional information kindly sent to me by Serge Kernbach:

1. "On metrology of systems operating with 'high-penetrating' emission" - This is the second part of the review - a survey on measurement of the emission (I'm finalizing now the third part, which is related to the same topic but in western history)
2. "Replication Attempt: Measuring Water Conductivity with Polarized Electrodes" - This is a JSE paper, where I was very curious about such an emission and made a large number of replications based on A.V.Bobrov approach
3."Long and Super-Long Range device-device and operator-device Interactions"- This paper is about our experiments (with colleagues) with long-range "non-local" signal transmission.

To quote from the last paper 3):

Long and Super-Long Range device-device and operator-device Interactions
Serge Kernbach, Vitaliy Zamsha, Yuri Kravchenko

Abstract - *This work describes performed device-device and operator-device experiments at long and super-long distances of >1 km, >100 km and >10000 km. Experimental setup uses two types of sensors, based on electric double layers and IGA-1 device, and two types of LED and laser generators. We analyzed the construction of the setup, establishing a connection between receiver and emitter, and multiple effects appeared. A common character of operator- and device- interactions is assumed. This approach can be considered as a novel communication system as well as a system for operator training with an objective feedback from devices.*

And here are examples of emitters used in these experiments*:*

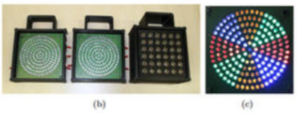


Figure 6. **(a)** Structure and **(b)** images of the LED and laser emitters without polymer cover; **(c)** polyspectral LED emitter.

© Association of Unconventional Science

LED and laser emitters

Arkadiusz Jadczyk

Arkadiusz Jadczyk is a theoretical physicist, and the husband of SOTT founder Laura Knight-Jadczyk.

Professor Jadczyk is fascinated by the problems of the foundations of quantum theory, and its relation to the philosophy of science and theories of knowledge, consciousness and mind. In the past he has worked on algebraic methods and the foundations of quantum theory, differential geometric methods of field theory, theories of gravitation, Kaluza-Klein theories of hidden dimensions, and supersymmetry, non-commutative geometry, fractals.

The interested reader can have a look at his Home Site and the Research Gate entry.

AJ- SOTT

How Google, Facebook and Twitter are already tricking you and manipulating your actual brainwaves!

Did you mean to turn yourself over to a faceless corporation to allow them to **manipulate you**, for their profit, like a **hard-wired zombie**? Did you mean to become a digital Stepford-Wife or a Yuppie Tool? Probably not, but you did. Here is how they do it to you, every single day, using a very insidious technology called "**Neuro-marketing**"-

Daniela Schiller, a Neuroscientist at the Mt. Sinai School of Medicine and an NYAS recipient of the Blavatnik Award for young scientists reveals the process in her article:

"**Yielding to Neural Temptation**

The personally tailored sponsored ads we receive daily on our computers are rather convenient. A delivery boy bringing the newspaper to our doorstep with all the relevant ads already circled could almost match the experience.

In a Hitchcock-like movie, newspaper ads would slowly creep into your house. As you sit on the sofa, an ad would instantly place itself under the palm of your hand. On one unfortunate occasion, you take a peek at it, and now it is devotedly following you around. Internet advertising reality is not that far from having a newspaper ad for a stalker. A friend confessed to me a few days ago that she owns "more than one pair of shoes that chased me around until I couldn't resist." When the distance between the tips of our fingers to an ad is so small, do we really make a choice when responding to it? Brain research suggests the opposite: The ad chooses us.

We feel uncomfortable learning that websites aggregate, profile, personalize and sell our information to third parties, but it takes us five minutes to get used to it. Mind reading has always been the most efficient way to communicate, and it feels just like it, when the shoes we were just thinking about appear in front of our eyes. Instead of us digging up information, information presents itself to us effortlessly. All we need is to choose, which we evidently do, or at least we believe we do.

Neuroscience researchers have a fairly good idea of how the brain reacts to stimuli imbued with motivational salience (such as ads, gift wraps, trademarks, warning signs, lottery cards, etc.) that signify outcomes of high value (such as a prizes, food, money, threats, etc.). A group of deep structures in the brain -- the basal ganglia -- is responsible for translating the information that motivational stimuli convey into choice. The basal ganglia mediate this process by forming an emotion-motor interface where reactions to motivating stimuli could guide actions. In a typical laboratory experiment, a rat learns to press a lever in order to drop food pellets into the food cup. The rat also learns, in a separate session, that whenever a stimulus such as a red light appears, food will drop into the cup. The interesting thing happens when the red light is turned on while the rat is pressing the lever: **The rat begins to press it more vigorously.** This is not very efficient on the rat's part. Each lever press delivers one food pellet, and pressing harder would not change the amount of food dropped into the cup, so why waste energy?

A study by Talmi and colleagues showed that people behave in much the same way as rats in the presence of motivational stimuli. Their study participants squeezed a handgrip in order to obtain money, and did it with greater vigor in the presence of money-related stimuli. This tells us that certain stimuli can invigorate our goal-directed actions just because they signal the same goal. If you have several goals in mind but can perform only one action at a given moment, what determines the action that would ultimately be chosen? We would like to think it is our ability to prioritize, but it could be something mundane as the little shoe image that appeared briefly at the corner of the screen, invigorating the must-buy-shoe-now action. Had it been a different image, you would have planned your vacation at the Bahamas right now. **Why might these efficient "reminders" for things we had on our mind anyway be problematic? The problem is that these salient stimuli do not only invigorate our actions; they also take control of the brain processing of our thoughts.**

In a study we performed in my lab, published recently in the journal Neuron, we examined the brain's reaction to such motivational stimuli. Instead of performing a real action, though, we asked the participants just to imagine the action. This type of motor imagery, such as picturing yourself throwing a ball, activates not only imagery networks but also motor regions that mediate real actions. The participants earned money for their imagery, which we tracked by measuring their brain responses in real time. In a separate session they also learned that a certain visual stimulus (such as a checkered square) signified winning money. This allowed us to create a laboratory experience that mimics your sitting by the computer, thinking of things you need to do, buy, or plan, when an ad appears on the screen. Here, we asked the participants to imagine that they were doing an action that would result in earning money, while the money-related visual stimulus appeared on the screen. Two interesting things happened in their brains.

First, we observed a boost in the neural responses of the motor imagery network. Second, the reward system of the brain, which encodes the value of the money-related stimuli, began working in coordination with the motor cortex. This neural synchronization between the "value" and "action" systems of the brain might be the gateway through which motivational stimuli act on our behavior. The motor cortex is the part of the brain that is in charge of commanding our body to perform actions. But here we engage it just by imagining an action we would have liked to perform. If the money-signaling stimulus appears while we imagine an action, the motor cortex receives a motivational cue from the reward system, and the two systems coordinate their function. This in turn could guide action selection, and determine which particular action we should execute.

Fast-forward into the future. Picture yourself sitting by your computer. Ads are appearing on the screen, and your thoughts are running in different directions. I am standing behind you, holding a device that measures your brain activation (Your mouse) . By observing the cascade of events that each ad triggers in your brain, I could tell which action you are going to perform before you actually perform it, maybe even before you are aware of it. **Neuro-marketing** companies would use the technology to identify the most effective ads, and which "teasers" they should plug in to stir your thoughts in a certain way. The more you obsess about something, the higher the chances of those ads causing the inevitable. Even if you try, just by exposing yourself to ads, you increase your chances of relapse. **You believe you bought those shoes because you made up your mind, but given the neural chain of events, someone elseprobably made up your mind for you**. The ads are there to tempt your neurons to fire in a certain way. They pave the path of your moment-to-moment decisions. This is how motivational stimuli, or advertising, works. We are surrounded by it every day. But when it is personally tailored to our brain, **our free will shrinks more effectively, placing us in the path to zombiness.**

There is nothing much to do about it now except avoiding ads, clearing browsing data, and trying not to think. The technology is there, and we want to stay connected. But now that we know how it works in our brain, we have a choice. We can honestly say that we choose to be manipulated."

Bradley Conners, expands: "The biggest secret of politics, and political strategists, is the knowledge that the majority of people are now medically, clinically, scientifically-provable brain damaged, ignorant lumbering shades of what people used to be.

The backers of Twitter, Facebook and Google can make you vote for who they say and buy what they have invested in. 2/3 of American voters are idiots. They are unable to exist without a programmed routine, unwilling to read the news and condemned to get all information from extremist talk shows that spout programmed lines over and over.

The Norman Rockwell icon of the “we are just plain folks in our overalls working hard on our farms” demographic of the average citizen is gone. Replaced by a drug addled, alcohol addled, Prozac addled, junk-food-brain-damaged horde of inner city gangsters, media catatonics, trophy wives, arrogant yuppie hipsters, obese pita-pocket gobbling, Jerry Springer addicts.

BILLBOARDS

In other words, a large number of the voting public are really, really dumb; Dumber than ever and easily brainwashed. They are increasing in numbers. The CIA discovered that you can brainwash some people in a matter of hours and most people in 5 days or less. Madison Avenue then perfected their techniques. “Over-messaging” is the intelligence agency technique of brainwashing an entire country (millions of people) over the course of a year or two, with subtle concept reinforcement. It is done in a way so that the population does not really notice it and so they think it was their idea. A successfully accomplished intelligence effort of this kind is called a “regime change” or “national transition effort”, on Madison Avenue it is called a: “marketing campaign”.

The increase in Reality TV shows about exceptionally stupid people has to do with the smart people turning off their TV’s and the dumb people increasing in numbers. The dumb ones are the only ones the TV networks can get to watch but they have to meet them on their level. Domestic education scores are dropping through the basement. Many high school students can’t read a book. The population is getting stupid at the speed of light. At college you can get smart but if you get too smart you might observe and realize all of the things in this essay are true so not everybody gets to go to college. If you aren’t addicted to something then you might see too clearly so the underwriting of the alcohol and drug industry continues (with your tax dollars) So you have the smart ones and the dumb ones (think Morlocks and Eloi) if you run the current cycles and patterns out into the future you might actually end up with Morlocks and Eloi. (If you still know how to read books you will know what this reference is, the rest of you: Google it) One wonders if the current fad about Zombies has to do with the public’s second sight on his potential future.

Political strategists exploit the dumb hordes by triggering their primal instincts using very base advertising concepts: “The bad guys will get you if you don’t vote for us” (Fear); “You won’t be able to get money to pay for your addictions if you don’t let us create the jobs” (Security); etc. An entire campaign can be won without the need to appeal to any intelligent voters. The bestial ones can bring in the majority more often than not. If you are reading this, you may be saying: “oh, I'm not one of them” but if you don’t read the news daily from multiple sources, if you only have products from the eye-level shelf at Safeway in your cupboards and if you watch “reality TV” shows… you just might be one. But you have one last chance to escape…"

Conners, a blogger goes on to say: “Ordinization: Manufactured Addiction For Profit. This is the process of using ingested substances to trick the brain in order to create addictive profit opportunity.

Fats, salts, sugars, breads, alcohol, tobacco and drugs use ordinization to addict consumers to buy them. Most of the makers of these products receive subsidies from your tax dollars. In other words, you are paying them to addict you and your family.

CARLOVE

The key to ordinization is that you don't want to believe it is happening to you because the addiction creates a synthetic bliss which your psychology causes you to defend. You get mad if someone implies they want to take away your cigarettes, alcohol, dessert, etc.

Government support of these products creates a nation of addicts, drunks, obese people, personality disorders, problem children and a very unhealthy society.

http://www.youtube.com/watch?v=W8EN4WctZuk

Billions of dollars are spent each year to refine and increase the addictive qualities of these products. "Product science" consultants have vast laboratories where they research food, beverage, fragrance, texture, taste and all human stimulants right down to each neuron in the brain. They want to see how they can control an entire generation of consumers to be unable to resist buying their product. Elite politician's operatives spray certain fragrances at rallies and then try to spray the same scent near polling places so you recall the candidate with a "home cooked meal" smell and want to vote for them without realizing why.

http://www.youtube.com/watch?v=KGlREiyrNF4

Vegas hotels and big Malls use psychological sense vapors to control consumers. 60 Minutes recently had a segment on a company, Givaudan, that other companies like McDonalds and Pepsi hire to create addictive flavors. This is all out in the marketplace. **If you don’t want to be a product zombie**, demand that Congress outlaw Ordinization.”

Could someone control your mind by simply aiming an electrical beam at you? Can you be turned from a lawn mowing yuppie into a neighborhood butchering madman in a few minutes? According to the articles above, and below, thanks to science, apparently so:

Ultrasound May Boost Brain's Performance, Study Finds

LiveScience | By Stephanie Pappas
Posted: 01/13/2014 8:10 am EST | Updated: 01/14/2014 2:44 pm EST

Smarter Ideas, Brain Disorders, Brain Initiative, Brain Science, Fetus, Brain Science, Sensory Perception, Ultrasound Brain, Ultrasound Brain Performance, Ultrasound Effects, Ultrasounds, Science News

Ultrasound may improve sensory perception, according to a new study in humans.

By directing ultrasound to a specific brain area, researchers were able to improve people's ability to discriminate between sensory inputs. Ultrasound is sound far above the upper limit of what humans can hear. It's useful in medical imaging. Doctors and technicians send bursts of ultrasound through tissue and record the echoes, creating a picture of what's inside — whether it's an injured knee or a fetus in utero.

Ultrasound also has potential for mapping the connectivity of the brain. Neuroscientists are particularly interested in understanding how brain areas chat with one another; in fact, a new federal project, the BRAIN Initiative, has the goal of mapping the healthy human brain. [Inside the Brain: A Photo Journey Through Time]

Ultrasound is one of several noninvasive methods that stimulate the brain. Another is transcranial magnetic stimulation, which stimulates the brain with magnets. A third is transcranial direct current stimulation, which uses electrodes to deliver a weak electrical current to the brain through the scalp.

The new study suggests that ultrasound may be the best of the bunch.

"We can use ultrasound to target an area of the brain as small as the size of an M&M," study researcher William Tyler, a neuroscientist at the Virginia Tech Carilion Research Institute, said in a statement. "This finding represents a new way of noninvasively modulating human brain activity with a better spatial resolution than anything currently available."

Surprising improvement

Tyler and his colleagues focused on sensory perception from the hand. They first placed an electrode on the wrist, over the nerve that carries impulses from the hand to the brain. Using a small electrical current, they stimulated that nerve while focusing ultrasound on the brain region that processes the nerve's signals.

The researchers recorded the participants' brain responses with electroencephalography (EEG), electrodes on the scalp that measure the electrical activity of the brain. The ultrasound weakened the brain waves that encode the tactile stimulation, they found.

But the next set of experiments revealed something truly strange.

The researchers conducted two tests of sensory perception. In the first, participants feel two pins against their skin and must distinguish whether they are being touched at one or two points. The closer the pins are to each other, the harder the task. In the second, researchers blow a series of air puffs against the participants' skin, and they must determine how many individual puffs they feel. The faster the puffs, the harder they are to discriminate.

Instead of these weak brain signals translating to poorer sensory perception, people's performance actually improved on both tests.

"Our observations surprised us," Tyler said. "Even though the brain waves associated with the tactile stimulation had weakened, people actually got better at detecting differences in sensations."

Tweaking the brain

What might explain this seeming paradox? The answer might have to do with how neurons function. When brain cells communicate, they can urge their neighbors to become active (excitation) or tell everyone to quiet down (inhibition). The ultrasound may have affected the brain region's balance of excitation and inhibition, Tyler said.

As a result, the excitation impulses may not have spread so far, essentially giving the brain a better triangulation of where the sensory inputs were coming from.

The boost in sensory perception vanished when researchers moved the ultrasound's focus just a half inch (1 centimeter). That means the method is a fine-grained way to "tweak" brain circuits, both to map their activity and potentially to treat brain disorders.

"In neuroscience, it's easy to disrupt things," said Tyler. "We can distract you, make you feel numb, trick you with optical illusions. It's easy to make things worse, but it's hard to make them better. These findings make us believe we're on the right path."

Follow Stephanie Pappas on Twitter and Google+. Follow us @livescience, Facebook & Google+. Original article on LiveScience.

China explores using stoplights for brain-hacking, to tell you what to think!

Imagine you pull up to an intersection as the light changes to red, as you wait for the light to change you suddenly decide you are hungry and want Dim Sum. You drive to the nearest Dim Sum and find that everybody else at that intersection has gone there too. Did you just get programmed by the LED stoplight with subliminal imaging?

At the next stop light will you suddenly decide that the Chairman of the Party is a "real sexy guy"? Did the stoplight put that thought in your mind? Did the stoplight tell you to be "obedient"?

Are those LED screens of sunsets and sunrises all over China only that.. or more? Tanya, at Live Science, describes the newly proven science to put images in your mind in a few milliseconds without you even being aware you got a message:

By Tanya Lewis, Staff Writer | January 17, 2014 12:00pm ET

The human brain can identify an image the eye has seen for only 15 milliseconds. Pin it

Credit: IKO, Shutterstock View full size image

The human brain can achieve the remarkable feat of processing an image seen for just 13 milliseconds, scientists have found. This lightning speed obliterates the previous record speed of 100 milliseconds reported by previous studies.

In the study, scientists showed people a series of images flashed for 13 to 80 milliseconds. Viewers successfully identified things like a "picnic" or "smiling couple" even after the briefest of glimpses.

"The fact that you can do that at these high speeds indicates to us that what vision does is find concepts," study leader Mary Potter, a professor of brain and cognitive sciences at MIT in Cambridge, Mass., said in a statement." That's what the brain is doing all day long — trying to understand what we're looking at." [10 Odd Facts About the Brain]

The eyes shift their gaze three times per second, so the ability to process images speedily may help the eyes find their next target, Potter said.

When a person looks at something, the retina sends that information to the brain, which processes shape, color and orientation. Potter and her team aimed to increase gradually the speed at which people could identify images until they were no more accurate than they would have been if they had guessed the image. The viewers had never seen the images before.

Previous studies suggested the brain takes at least 50 milliseconds to send visual information from the retina to the "top" of the brain's visual processing chain and back again in loops that confirm what the eye saw, so the researchers expected people would get worse at seeing images shown for less than 50 milliseconds.

But Potter's team found that although people's performance declined on average as the time was reduced, they still performed better than chance when identifying images flashed for as little as 13 milliseconds, the speed limit of the computer monitor they used.

The findings, detailed online Jan. 16 in the journal Attention, Perception, and Psychophysics, show that people were processing the images much more quickly than scientists believed was possible. One reason may be that the study participants became faster with practice, and also received feedback on their performance, Potter said.

The findings support those from a study of macaque monkeys in 2001 that found the animals respond to specific kinds of images — such as faces — flashed for just 14 milliseconds.

These studies demonstrate that the information only needs to flow in one direction, from the retina to the visual brain areas, in order to identify concepts, without needing feedback from other brain areas. This ability could give the brain the time it needs to decide where to point the eyes, which can take only 100 to 140 milliseconds. (It might also explain why some people report a "sixth sense," when they unconsciously pick up on visual cues in a scene.)

In addition, even though viewers saw the images for only 13 milliseconds, part of their brain may have continued to process them, because sometimes, participants weren't asked about the image until after they saw a sequence of images.

Next, the researchers want to see how long the brain can hold visual information glimpsed for such a short time, and which brain regions are active when a person correctly identifies what they saw.

Follow Tanya Lewis on Twitter and Google+. Follow us @livescience, Facebook & Google+. Original article on LiveScience.

Announcing: The World's Most Hacker Proof Technology On the Planet!!!

The Tuskegee Hyper Vault.
Over 1000 years in development.!!!!!!!

Formerly known as a "Yellow Legal Pad", this shocking innovation has now been tested and **PROVEN** to be impenetrable. No living computer hacker **ANYWHERE ON EARTH** can hack this device!

Brought to you by the amazing scientists at ACS (Any Commonsense Solution), this device will soon be available nationwide, and even in France.

ACS is about to reveal an even more incredible technology: "**The Manila File Folder**."

This device promises to double the already awesome invisibility and stealth mode sub-zero incredible-ness of **The Tuskegee Hyper Vault!!**

Just when we thought technology was our worst enemy, it gives us a gift from heaven.
We have obtained this exclusive image of the unit:

legal-pad

How The NSA Hacks Your iPhone (Presenting DROPOUT JEEP)

Submitted by Tyler Durden on 12/30/2013 12:22 -0500

- Apple
- ETC
- PrISM
- SPY
- Steve Jobs

Following up on the latest stunning revelations released yesterday by German Spiegel which exposed the spy agency's 50 page catalog of "backdoor penetration techniques", today during a speech given by Jacob Applebaum (@ioerror) at the 30th Chaos Communication Congress, a new bombshell emerged: specifically the complete and detailed description of how the NSA bugs, *remotely*, your iPhone. The way the NSA accomplishes this is using software known as Dropout Jeep, which it describes as follows: "**DROPOUT JEEP is a software implant for the Apple iPhone that utilizes modular mission applications to provide specific SIGINT functionality. This functionality includes the ability to remotely push/pull files from the device. SMS retrieval, contact list retrieval, voicemail, geolocation, hot mic, camera capture, cell tower location, etc. Command, control and data exfiltration can occur over SMS messaging or a GPRS data connection.** All communications with the implant will be covert and encrypted."

The flowchart of how the NSA makes your iPhone its iPhone is presented below:

- NSA ROC operator
- Load specified module
- Send data request
- iPhone accepts request

- Retrieves required SIGINT data
- Encrypt and send exfil data
- Rinse repeat

And visually:

What is perhaps just as disturbing is the following rhetorical sequence from Applebaum:

> "Do you think Apple helped them build that? I don't know. I hope Apple will clarify that. Here's the problem: **I don't really believe that Apple didn't help them,** I can't really prove it but [the NSA] literally claim that anytime they target an iOS device that it will succeed for implantation. Either they have a huge collection of exploits that work against Apple products, meaning that they are hoarding information about critical systems that American companies produce and sabotaging them, **or Apple sabotaged it themselves**. Not sure which one it is. I'd like to believe that since Apple didn't join the PRISM program until ***after*** Steve Jobs died, that maybe it's just that they write shitty software. We know **that's** true."

Or, Apple's software is hardly "shitty" even if it seems like that to the vast majority of experts (kinda like the Fed's various programs), and in fact it achieves precisely what it is meant to achieve.

Either way, now everyone knows that their iPhone is nothing but a gateway for the NSA to peruse everyone's "private" data at will. Which, incidentally, is not news, and was revealed when we showed how the "NSA Mocks Apple's "Zombie" Customers; Asks "Your Target Is Using A BlackBerry? Now What?""

How ironic would it be if Blackberry, left for dead by virtually everyone, began marketing its products as the only smartphone that **does not allow the NSA access to one's data** (and did so accordingly). Since pretty much everything else it has tried has failed, we don't see the downside to this hail mary attempt to strike back at Big Brother and maybe make some money, by doing the right thing for once.

We urge readers to watch the full one hour speech by Jacob Applebaum to realize just how massive Big Brother truly is, but those who want to just listen to the section on Apple can do so beginning 44 minutes 30 seconds in the presentation below.

----

http://www.youtube.com/watch?v=qAT_ina93NY

http://www.youtube.com/watch?v=_YffwdsnKXo

USER ARTICLES FOR THE INVESTIGATION:

Put each **Article Title** in the search window at the top right of the page to source the original:

- Snowden docs expose Match.com/OK Cupid and big dating sites as fronts for honey traps and privacy harvesting.2014/02/08
- CES 2014: Why is it still a “festival of corporate spying and privacy invasion”?2014/01/08
- THE PRIVACY RIGHTS INVESTIGATIONPage
- Tesla Owner Buyers List Out in the Public. No privacy for Tesla Owners!2013/05/23
- Europe and Asia launch WAR on Google, Facebook, Amazon mind-control digital onslaught!2014/07/06
- THE GOOGLE INVESTIGATIONPage
- THE BATTERY INVESTIGATIONPage
- INVESTIGATIONSPage
- Why so Many Tesla Drivers Turn Out to Be Deviants…Page
- GOP web gurus: “We lost last election because Google is already using Facebook’s “Mood Manipulation” tricks on voters but PAYBACK has already begun”2014/07/02
- Do FACEBOOK’s megalomaniac billionaire investors have a secret plan to destroy free will? The FACEBOOK “Mood Manipulation” programs.2014/07/01
- Is MATCH.COM using RACISM and FACE-ISM by using facial recognition software to data-mine you?2014/06/23
- FACEBOOK AND GOOGLE HAVE BEEN DOING MANIPULATIVE EXPERIMENTS ON YOU EVER SINCE THEY WERE STARTED. MOOD & THOUGHT MANIPULATION HAVE BEEN ONGOING AT GOOGLE AND FACEBOOK FOR YEARS! PSYOPS FOR PROFIT AND POLITICS2014/06/16
- RED ALERTSPage
- How your enemies can have you attacked on “data-mining” services? Every time you touch a keyboard, you hand your opposition the tools of your own destruction!2014/06/10
- PUBLIC TO TECH COMPANIES: “SCREW YOU!” $100 Billion in losses and counting… Consumers are fed up!2014/06/08
- CARGATE INTERACTIVE PUBLIC TIMELINE: CAR-GATE ENERGY DEPT. SCANDALPage
- Department of Energy Head announces he engaged in “Meticulous Due Diligence” to ensure that only campaign billionaire funders got DOE funding!2014/06/05
- Are Amazon, Google, Facebook and Twitter under big-time investigation?2014/06/04
- NEVER PUT YOUR PICTURE ON THE INTERNET! Why? DATA-MINING OF KIDS AND Because of things like this:2014/06/01
- Does Axciom rob your soul every minute of every day? Data broker rape!2014/06/01
- How CISCO Screwed the Pooch: The Built-in Backdoors-of-doom!2014/06/01
- Over 1000 Reason’s Why Lithium-ion Is a DEADLY, CRIMINAL, VERY BAD THING!2014/05/16
- The First Public RICO (Corruption/Racketeering) internet lawsuit goes online2014/05/15
- Who watches the watchers? Big Data goes unchecked2014/05/15
- “YOU CAN MAKE MORE MONEY OFF OF PREGNANT WOMEN!”2014/05/12
- MATCH.COM, OK CUPID, PLENTY OF FISH, AND SIMILAR DATING FACTORYSITES, SPY ON YOU!2014/05/09
- How to survive the internet!2014/03/25
- THE AFGHANI-SCAM INVESTIGATIONPage
- What if there is no NSA! ? Is it all just a practical joke on Silicon Valley campaign $$2014/03/19
- Additional Tesla Articles- Section 1APage
- INVESTIGATING TESLA MOTORS – PART BPage
- CARGATE! Billions of dollars in kick-backs from taxpayer $$Page
- You say you “don’t care if you are being watched online”, Here’s why you MUST CARE:2014/03/17
- The Next Generation of Hacker-Proof Technology Has Arrived!2014/02/24
- The Green mobsters of the 1% and their Divine Disinformation Campaigns2014/02/19
- How social media companies brain-wash you and steal your future!2014/02/19
- Are specific politicians using the NSA for private personal vendetta’s and to hit their business competitors?2014/02/02
- Who controls the Department the of Energy?2014/01/28
- “The Archangel Linkages”: A film more real than film?2014/01/24
- Is it just a misunderstanding to think that “Google is Evil”?2014/01/23
- What are the biggest fears about the spying scandal?2014/01/18
- Are Google, Facebook and Twitter, per Reddit, a “Cartel of evil” or just a fun bunch of Stanford buddies?2014/01/14
- Got a Pulitzer? Now YOU can get your own Billionaire! Start a New News Outlet. Be Revolting.. err.. a revolter..2014/01/10
- The Death of the Internet – The Dawn of the PUBLI-NET: 1.1.142013/12/27
- How Washington DC Politicos Have Reporters “HIT” and Intimidated!Page
- THE INSIDE TESLA INVESTIGATIONPage
- How F**KED Over By Your Own Representatives Do you Need To Get Before You Get Upset?Page

- ACTUAL CRIMES! And the indictments go to…..Page
- Tesla hiding reports of multiple defects of Tesla Cars?!Page
- TSLA Tesla Stock. “Shill”, Fake, “Pump” and manipulate tech stocks with tax $$$!Page
- Tesla TOXIC SMOKE! THE FACTS ON TESLA FIRES:Page
- Tesla Driver “Douche Bag” Controversy. Are Tesla drivers inherently unsafe?Page
- Tesla investor/campaign donors paid back with free luxury jet fuel, NASA contracts, patent laws, etc…Page
- The Character Assassination of Martin Eberhard by Elon MuskPage
- Tesla’s Musk hates unions. Employee Compensation, “Spying on employees” and Safety Issues At TeslaPage
- Multiple Fraud and Malfeasance Lawsuits Against TeslaPage
- TESLA SAFETY REPORT Vers. 1.05M- Public Wiki Produced for NHTSA and other governmental agencies2013/12/06
- Senate Ethics Committee accuses DOJ, FBI, IRS of investigation cover-up!Page
- FEATURES: HOT TOPICSPage
- THE ORGANIZED CRIME IN PUBLIC OFFICE INVESTIGATIONPage
- THE VENTURE CAPITAL INVESTIGATIONPage
- Lobbying With BribesPage
- Online Dating Service Corruption: Date Rape and Data RapePage
- COVER-UP!!!!!!!!!!!!!!!!!!!!!!!!!!!!2013/12/01
- ABOUTPage
- Spying Controversy Blowback, The Rebekah Brooks Trial and Dianne Feinstein2013/10/28
- Does the President’s Staff Just Sit Around and Lie To Him All Day Long? White House: Fire Some People!2013/10/24
- Steven Chu and The Big Screw! FOLLOW THE MONEY…2013/09/19
- Bundlers and DOE Ex-Staff find that the tracks they thought they covered up were actually NOT covered up… Oops!2013/09/01
- Deaths, so far, In These Scandals! Murders and Acquisitions?2012/10/31