Tomgram: Peter Van Buren, *1984* Was an Instruction Manual

Posted by Peter Van Buren at 8:13am, December 3, 2013.
Follow TomDispatch on Twitter @TomDispatch.

[Note for TomDispatch Readers: *A little bit of good news about our publishing program. Our first original book,* They Were Soldiers: How the Wounded Return From America's Wars -- The Untold Story *by Ann Jones, is now going into its second printing! That's, in part, thanks to your support in buying copies. If you meant to, but haven't yet done so and are an Amazon customer, please click the above link, or rush out to your nearest independent bookstore and get a copy. It will genuinely make a difference to our publishing future if this book succeeds. Tom*]

Once upon a time, you might have said that someone "disappeared." But in the 1970s in Argentina, Chile, and elsewhere, that verb grew eerily more active in its passive form. He or she no longer "disappeared," but "*was* disappeared" -- up to 30,000 Argentineans by their own military in the course of an internal struggle that came to be known as "the dirty war." Those gone were the "*desaparecidos.*"

There is something so deeply, morally repugnant about disappearing another human being, no matter how or where or why it's done, that it's hard to express. Yet in twenty-first century America, the possibilities for disappearing people in new and inventive ways may be migrating online, as former State Department whistleblower and TomDispatch regular Peter Van Buren suggests in his latest post. *Tom*

Welcome to the Memory Hole

Disappearing Edward Snowden

By Peter Van Buren

What if Edward Snowden was made to disappear? No, I'm not suggesting some future CIA rendition effort or a who-killed-Snowden conspiracy theory of a disappearance, but a more ominous kind.

What if everything a whistleblower had ever exposed could simply be made to go away? What if every National Security Agency (NSA) document Snowden released, every interview he gave, every documented trace of a national security state careening out of control could be made to disappear in real-time? What if the very posting of such revelations could be turned into a fruitless, record-less endeavor?

Am I suggesting the plot for a novel by some twenty-first century George Orwell? Hardly. As we edge toward a fully digital world, such things may soon be possible, not in science fiction but in our world -- and at the push of a button. In fact, the earliest prototypes of a new kind of "disappearance" are already being tested. We are closer to a shocking, dystopian reality that might once have been the stuff of futuristic novels than we imagine. Welcome to the memory hole.

Even if some future government stepped over one of the last remaining red lines in our world and simply assassinated whistleblowers as they surfaced, others would always emerge. Back in 1948, in his eerie novel *1984*, however, Orwell suggested a far more diabolical solution to the problem. He conjured up a technological device for the world of Big Brother that he called "the memory hole." In his dark future, armies of bureaucrats, working in what he sardonically dubbed

the Ministry of Truth, spent their lives erasing or altering documents, newspapers, books, and the like in order to create an acceptable version of history. When a person fell out of favor, the Ministry of Truth sent him and all the documentation relating to him down the memory hole. Every story or report in which his life was in any way noted or recorded would be edited to eradicate all traces of him.

In Orwell's pre-digital world, the memory hole was a vacuum tube into which old documents were physically disappeared forever. Alterations to existing documents and the deep-sixing of others ensured that even the sudden switching of global enemies and alliances would never prove a problem for the guardians of Big Brother. In the world he imagined, thanks to those armies of bureaucrats, the present was what had always been -- and there were those altered documents to prove it and nothing but faltering memories to say otherwise. Anyone who expressed doubts about the truth of the present would, under the rubric of "thoughtcrime," be marginalized or eliminated.

Government and Corporate Digital Censorship

Increasingly, most of us now get our news, books, music, TV, movies, and communications of every sort electronically. These days, Google earns more advertising revenue than all U.S. print media combined. Even the venerable *Newsweek* no longer publishes a paper edition. And in that digital world, a certain kind of "simplification" is being explored. The Chinese, Iranians, and others are, for instance, already implementing web-filtering strategies to block access to sites and online material of which their governments don't approve. The U.S. government similarly (if somewhat fruitlessly) blocks its employees from viewing Wikileaks and Edward Snowden material (as well as websites like TomDispatch) on their work computers -- though not of course at home. Yet.

Great Britain, however, will soon take a significant step toward deciding what a private citizen can see on the web even while at home. Before the end of the year, almost all Internet users there will be "opted-in" to a system designed to filter out pornography. By default, the controls will also block access to "violent material," "extremist and terrorist related content," "anorexia and eating disorder websites," and "suicide related websites." In addition, the new settings will censor sites mentioning alcohol or smoking. The filter will also block "esoteric material," though a UK-based rights group says the government has yet to make clear what that category will include.

And government-sponsored forms of Internet censorship are being privatized. New, off-the-shelf commercial products guarantee that an organization does not need to be the NSA to block content. For example, the Internet security company Blue Coat is a domestic leader in the field and a major exporter of such technology. It can easily set up a system to monitor and filter all Internet usage, blocking web sites by their address, by keywords, or even by the content they contain. Among others, Blue Coat software is used by the U.S. Army to control what its soldiers see while deployed abroad, and by the repressive governments in Syria, Saudi Arabia, and Burma to block outside political ideas.

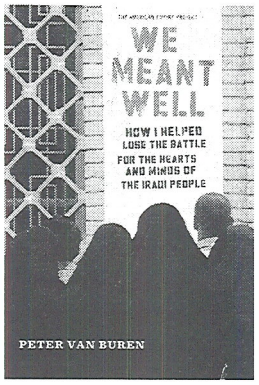
Google Search...

In a sense, Google Search already "disappears" material. Right now Google is the good guy vis-à-vis whistleblowers. A quick Google search (0.22 seconds) turns up more than 48 million hits on Edward Snowden, most of them referencing his leaked NSA documents. Some of the websites display the documents themselves, still labeled "Top Secret." Less than half a year ago, you had to be one of a very limited group in the government or contractually connected to it to see such things. Now, they are splayed across the web.

Google -- and since Google is the planet's number one search engine, I'll use it here as a shorthand for every search engine, even those yet to be invented -- is in this way amazing and looks like a massive machine for spreading, not suppressing, news. Put just about anything on

the web and Google is likely to find it quickly and add it into search results worldwide, sometimes within seconds. Since most people rarely scroll past the first few search results displayed, however, being disappeared already has a new meaning online. It's no longer enough just to get Google to notice you. Getting it to place what you post high enough on its search results page to be noticed is what matters now. If your work is number 47,999,999 on the Snowden results, you're as good as dead, as good as disappeared. Think of that as a starting point for the more significant forms of disappearance that undoubtedly lie in our future.

Hiding something from users by reprogramming search engines is one dark step to come. Another is actually deleting content, a process as simple as transforming the computer coding behind the search process into something predatory. And if Google refuses to implement the change-over to "negative searches," the NSA, which already appears to be able to reach inside Google, can implant its own version of malicious code as it has already done in at least 50,000 instances.



Buy the book

But never mind the future: here's how a negative search strategy is already working, even if today its focus -- largely on pedophiles -- is easy enough to accept. Google recently introduced software that makes it harder for users to locate child abuse material. As company head Eric Schmidt put it, Google Search has been "fine-tuned" to clean up results for more than 100,000 terms used by pedophiles to look for child pornography. Now, for instance, when users type in queries that may be related to child sexual abuse, they will find no results that link to illegal content. Instead, Google will redirect them to help and counseling sites. "We will soon roll out these changes in more than 150 languages, so the impact will be truly global," Schmidt wrote.

While Google is redirecting searches for kiddie porn to counseling sites, the NSA has developed a similar ability. The agency already controls a set of servers codenamed Quantum that sit on the Internet's backbone. Their job is to redirect "targets" away from their intended destinations to websites of the NSA's choice. The idea is: you type in the website you want and end up somewhere less disturbing to the agency. While at present this technology may be aimed at sending would-be online *jihadis* to more moderate Islamic material, in the future it could, for instance, be repurposed to redirect people seeking news to an Al-Jazeera lookalike site with altered content that fits the government's version of events.

...and Destroy

However, blocking and redirecting technologies, which are bound to grow more sophisticated, will undoubtedly be the least of it in the future. Google is already taking things to the next level in the service of a cause that just about anyone would applaud. They are implementing picture-detection technology to identify child abuse photographs whenever they appear on their systems, as well as testing technology that would remove illegal videos. Google's actions against child porn may be well intentioned indeed, but the technology being developed in the service of such anti-child-porn actions should chill us all. Imagine if, back in 1971, the Pentagon Papers, the first glimpse most Americans had of the lies behind the Vietnam War, had been deletable. Who believes that the Nixon White House wouldn't have disappeared those documents and that history wouldn't have taken a different, far grimmer course?

Or consider an example that's already with us. In 2009, many Kindle owners discovered that Amazon had reached into their devices overnight and remotely deleted copies of Orwell's *Animal Farm* and *1984* (no irony intended). The company explained that the books, mistakenly "published" on its machines, were actually bootlegged copies of the novels. Similarly, in 2012, Amazon erased the contents of a customer's Kindle without warning, claiming her account was "directly related to another which has been previously closed for abuse of our policies." Using the

same technology, Amazon now has the ability to replace books on your device with "updated" versions, the content altered. Whether you are notified or not is up to Amazon.

In addition to your Kindle, remote control over your other devices is already a reality. Much of the software on your computer communicates in the background with its home servers, and so is open to "updates" that can alter content. The NSA uses malware -- malicious software remotely implanted into a computer -- to change the way the machine works. The Stuxnet code that likely damaged 1,000 centrifuges the Iranians were using to enrich uranium is one example of how this sort of thing can operate.

These days, every iPhone checks back with headquarters to announce what apps you've purchased; in the tiny print of a disclaimer routinely clicked through, Apple reserves the right to disappear any app for any reason. In 2004, TiVo sued Dish Network for giving customers set-top boxes that TiVo said infringed on its software patents. Though the case was settled in return for a large payout, as an initial remedy, the judge ordered Dish to electronically disable the 192,000 devices it had already installed in people's homes. In the future, there will be ever more ways to invade and control computers, alter or disappear what you're reading, and shunt you to sites weren't looking for.

Snowden's revelations of what the NSA does to gather information and control technology, which have riveted the planet since June, are only part of the equation. How the government will enhance its surveillance and control powers in the future is a story still to be told. Imagine coupling tools to hide, alter, or delete content with smear campaigns to discredit or dissuade whistleblowers, and the power potentially available to both governments and corporations becomes clearer.

The ability to move beyond altering content into altering how people act is obviously on governmental and corporate agendas as well. The NSA has already gathered blackmail data from the digital porn viewing habits of "radical" Muslims. The NSA sought to wiretap a Congressman without a warrant. The ability to collect information on Federal judges, government leaders, and presidential candidates makes J. Edgar Hoover's 1950s blackmail schemes as quaint as the bobby socks and poodle skirts of that era. The wonders of the Internet regularly stun us. The dystopian, Orwellian possibilities of the Internet have, until recently, not caught our attention in the same way. They should.

Read This Now, Before It's Deleted

The future for whistleblowers is grim. At a time not so far distant, when just about everything is digital, when much of the world's Internet traffic flows directly through the United States or allied countries, or through the infrastructure of American companies abroad, when search engines can find just about anything online in fractions of a second, when the Patriot Act and secret rulings by the Foreign Intelligence Surveillance Court make Google and similar tech giants tools of the national security state (assuming organizations like the NSA don't simply take over the search business directly), and when the sophisticated technology can either block, alter, or delete digital material at the push of a button, the memory hole is no longer fiction.

Leaked revelations will be as pointless as dusty old books in some attic if no one knows about them. Go ahead and publish whatever you want. The First Amendment allows you to do that. But what's the point if no one will be able to read it? You might more profitably stand on a street corner and shout at passers by. In at least one easy-enough-to-imagine future, a set of Snowden-like revelations will be blocked or deleted as fast as anyone can (re)post them.

The ever-developing technology of search, turned 180 degrees, will be able to disappear things in a major way. The Internet is a vast place, but not infinite. It is increasingly being centralized in the hands of a few companies under the control of a few governments, with the U.S. sitting on the major transit routes across the Internet's backbone.