Should journalism be a surveillance-safe space?
Ethan Zuckerman, December 2014

It has rapidly become conventional wisdom that the documents about NSA surveillance released by Edward Snowden constitute a turning point in public dialog about rights and privacy in a digital age. The Snowden revelations may also represent a turning point in journalism, illuminating the need for investigative journalism to be supported by robust legal protections, while also suggesting that most contemporary newsrooms are not ready to defend against sustained, aggressive, well-resourced surveillance. Journalism post-Snowden will need to become more technically savvy, more sensitive to risks to sources, and more aware of surveillance and privacy as a beat readers wish to read about.

But in civic and political senses, it is less clear that Snowden’s revelations and the accompanying reporting have been as pivotal as the former security consultant had hoped. While there’s been a great deal of discussion regarding government invasion of privacy, it is not at all clear that significant policy changes are forthcoming, or that revelations have energized a sustained movement focused on protecting citizens against the abuses Snowden has warned against, at least within the United States. The public reaction to widespread surveillance has been, in many quarters, a resigned shrug, an acceptance that this is simply how things are on the internet. This essay explores the manufacture of the apathy towards normalized surveillance, and the small but significant role major journalistic outlets have played in cultivating this apathy, in the hopes of persuading journalistic leaders to take up the protection of reader privacy as part of their civic mission.

The least surprising surprise

Unpacking the mixed responses to the Snowden revelations might start from a simple, if somewhat contrary, observation: the government and private surveillance Snowden and collaborators revealed was one of the world’s least surprising surprises. For many years, scholars of internet security have been split into roughly two camps regarding online surveillance: those that believed that a select set of governments were practicing mass data collection online and investing significant resources in compromising specific targets, and a more paranoid set, who believed the US was likely to be one of these governments. The most paranoid in this community consistently warned that the US could and would use massive computational power and unclear legal frameworks to put millions of Americans and users of American internet services under surveillance. Apparently paranoid security professionals like Jacob Appelbaum, who saw the US as a likely adversary even before he began working with Wikileaks, got it right and the rest of us got it wrong.¹

It wasn't a surprise that governments were capable of extremely sophisticated electronic surveillance. Research conducted by groups like Citizen Lab¹¹ had extensively documented the capabilities of software like FinFisher, designed to
allow law enforcement officials to target the communications of criminal suspects, but widely speculated to be used by repressive governments to surveil dissidents and political activists. Widespread, sweeping surveillance of social media is a technique scholars had seen as well, with Tunisian intelligence officials intercepting user logins to Facebook so they could read the messages of thousands of users of those systems. What was surprising was that widespread electronic surveillance was taking place in a democracy where we would expect more oversight and scrutiny. For some, the most surprising aspect was not that US intelligence agencies were surveilling users of US services, but that US corporations were providing those agencies with access to their systems. Again, the most paranoid had long observed that these platforms were vulnerable to discovery through subpoena or other means - those who were surprised expected that the owners of these platforms would have put up more of a fight.

In the wake of Snowden's revelations and the accompanying reporting, a set of diverse commentaries appeared with variants on the same headline: "Why is anyone surprised?" Some were knowing pieces from intelligence insiders and security experts who made clear that they were aware of the government’s capabilities. But other commenters argued that anyone who had been watching the expansion of US government security powers under the PATRIOT act should have anticipated precisely this sort of overreach. A cynical and worldly undertone in these stories suggests that anyone who did find massive metadata collection surprising simply hadn’t been paying close enough attention, or was a naïf.

The Snowden revelations were also unsurprising in a structural way. They followed an established model of how a whistleblower story unfolds in the press. As with the Wikileaks documents revealed by Chelsea Manning, a massive collection of apparently important documents were released by a whistleblower, whose character, personality and motivations became a storyline in themselves. The documents themselves were intriguing, but near incomprehensible, a stew of codewords and acronyms that demanded deep investigation by experts and careful interpretation and storytelling from skilled journalists. (While the Pentagon Papers as revealed by Daniel Ellsberg were an easier read than the Wikileaks or NSA document caches, emergence of Ellsberg as a story in and of himself and the use of the Pentagon Papers as jumping off point for journalistic analysis of the US role in Southeast Asia suggest this model of journalistic response goes back at least 40 years.)

Because the revelations were deeply uncomfortable for the US and UK governments, these journalistic interpreters needed one of the most powerful features of the professional newsroom: a strong legal team to ensure they would be allowed to publish what they discovered. The Guardian documented a set of actions and threats made by the UK government - the detention of David Miranda, Glenn Greenwald's partner and document courier, threats of police raids and invocation of the Official Secrets Act - which led the newspaper to destroy the files containing the Snowden documents rather than give the hard drives that contained them to UK authorities.
The heavy-handed UK government response was a reminder that we need strong, independent journalism in a digital age, where organizations have the fiscal resources to invest in significant investigation and the legal backing to make publication possible.

This reminder of the importance of the newspaper's civic role as a principled opponent of the government, when necessary, might be seen as a reassurance to the otherwise uncomfortable reminder that Snowden sought out an activist filmmaker and a highly opinionated advocacy journalist to offer his revelations, out of concern that traditional newsrooms might not pursue the story and might not have the technical chops to pursue the story carefully. While the Guardian and the Washington Post surely deserve the Pulitzer prize for public service for their brave, careful reporting, it is also possible to see the award as the industry reassuring itself of its continued importance, and of the continued validity of a model of journalism that interprets complex stories to the general public.

For some, the biggest surprise of the Snowden revelations is that they have not led to a broad public movement against surveillance in the United States. Instead, surveillance has become an issue on which the American population seems neatly split and not on conventional party lines. Libertarian Rand Paul has been a vocal advocate against surveillance, while democratic leaders like Nancy Pelosi have been sharply critical of Snowden's actions. It is perhaps unsurprising that a mainstream protest movement has not emerged given that neither party has embraced it as a campaign issue. The White House’s dismissal of the Amash-Conyers amendment and halting response to the Review Group on Intelligence and Communications Technologies recommendations has made it difficult for Democratic leaders to take a strong stand against surveillance, while a tendency towards favoring military security over personal rights makes it challenging for Republicans to demand surveillance reforms.

This slow and partial governmental response may point to the structural limits of whistleblowing as a force for change. When whistleblowing leads to reporting which leads to congressional investigation and pressure, or embarrasses the executive branch into action, it is a powerful tool for individuals and the press to seek change. But without strong reactions within the executive and legislative branches, substantial change may not happen without a sustained popular movement. US and UK newspapers are traditionally more comfortable pressuring elected representatives than serving as organizers of citizen movements. It is possible that Edward Snowden had hoped that Poitras and Greenwald could take a less conventional role and serve as heads of this movement, and Poitras's documentary "Citizenfour" may become the rallying point for that movement. But thus far, readers of these stories who experienced a sense of outrage have little to do to channel their rage, as it is unclear that meaningful action will be taken or how a citizen could effectively make change on these issues. This scenario is tragically unsurprising, as paralysis of US government at legislative and executive levels, and
resulting closure of paths towards citizen pressure and engagement, has become a recurrent 21st century pattern.

The model that makes us expect surveillance

Another possible explanation for the fact that Snowden revelations haven't generated a broad public movement is that we may simply expect to be surveilled when we interact online. The dominant online business model to support content and services is one in which we trade our attention for content and services. This model is the response to the fact that, in the mid-1990s, it was difficult to charge users for subscriptions and impossible to charge for micropayments. The advent of web banner ads as an easily implemented revenue source for pioneering web firms created a culture where advertising, rather than subscription revenue was the default. The popularity of this model trained early adopters of the web to assume that content and services would be free, subsidized by advertising.

Unfortunately, this has turned out to be fiscally challenging for publishers as a user's attention appears to be worth significantly less online than offline. Felix Stadler used a set of back of the envelope calculations to determine that Facebook captured 20 hours a month of users attention, but that Facebook was able to yield only $0.20 per month for marketing that attention to advertisers. By contrast, Don Marti calculates (using similar methods) that print newspapers capture 7 hours of user attention per month, but that this attention is worth four times as much to advertisers. An "attention minute" is worth more than ten times more on a paper publication than online, despite the fact that ads in a newspaper can't lead a viewer directly to more information or to a transaction. At present, advertisers are treating print and digital advertisements as different products: they appear willing to pay for the "brand building" aspects of advertising offline but not online.

This "paper dollars, digital dimes" problem has led to a wave of businesses working to improve the dismal performance of online ads, most often by collecting additional information about the viewer of a page. Advertising networks set "cross-site cookies" which track a user's movements between websites, hoping to generate psychographic data about the viewer based on what sites she visits. Other techniques like browser fingerprinting attempt to overcome the web's structural anonymity and identify each web browser with a unique signature determined from information that browser leaks to the website it interacts with (screen size, fonts installed, version numbers, plugins and other apparently innocuous data are combined into a profile that is difficult to disguise and highly likely to be unique.) Social networks like Facebook collect a wealth of personal data on users, then complement these rich profiles with behavioral data (who we interact with, what we post about) to offer yet richer targeting data. Even with this data, Facebook ads are worth less than print ads, leading startup companies to promise yet more invasive forms of surveillance and targeting, leading Jeff Hammerbacher, an early Facebook employee (and early defector from the company) to observe "The best minds of my generation are thinking about how to make people click ads."
It is extremely difficult to avoid this sort of surveillance. The sorts of techniques Snowden used to contact Poitras and pass documents to her is powerful enough to defeat a technique like browser fingerprinting, but is well outside the skillset of most internet users. (It also makes more social media tools entirely unusable, as Tor, the toolset used to disguise a user’s IP address, requires a user to turn off Javascript, the language used to make the interface for social media tools interactive.) A savvy and determined user might use ad filtering software like AdBlock Plus (which advertises a userbase of 21 million per day\textsuperscript{xvi}) and an additional tool like Privacy Badger (which boasts only 150,000 installs\textsuperscript{xxvii}) to block third party cookies, but these users are a tiny minority of online users. (Ghostery, a popular service to block third-party cookies, claims 20 million users\textsuperscript{xxviii}, while Tor has approximately 2 million daily users\textsuperscript{xxix}) Helen Nissenbaum, a philosopher of technology and privacy, suggests that this problem may be best solved by flooding sites and ad networks with bogus data, obscuring a user’s searches in a wave of algorithmically generated cover traffic. (Nissenbaum’s newest tool, Ad Nauseum, confronts the absurdities of internet advertising head on, blocking all ads on a webpage from a user’s view, while registering a click on each ad, attempting to bankrupt advertisers, who pay per click.\textsuperscript{xx})

If we assume that users of tools like Ghostery are also blocking ads with Ad Blocker Plus, roughly 0.7% of internet users are taking significant steps to protect their online privacy. Since the vast majority of web users do not take these unusual steps to frustrate commercial surveillance, we might conclude that they are either unaware that surveillance takes place, or do not feel like such surveillance is avoidable. Pew Research’s Privacy Panel Survey conducted in January of 2014 suggests that the latter is much more likely that the former, as 50% of people who said they did not know much about government surveillance programs, and 61% of those who were well informed about surveillance, did not see their social network communications as secure.\textsuperscript{xix} But another dynamic may be at play as well. danah boyd, a leading researcher on youth behavior online, reports that the young people she interviews tell her they prefer ad-supported tools because they know those tools will remain free for them to use.\textsuperscript{xviii} Consciously or not, these users have accepted the bargain "if you’re not paying for something, you’re the product, not the customer.

This dynamic may be changing. When nascent social network Ello advertised that it planned on building a Facebook competitor that was not based on targeted advertising, it was swamped by requests for accounts.\textsuperscript{xiii} That an absence of targeting was the network’s chief selling point makes clear how firmly surveillance has been established as the default. That there’s not massive pressure on Facebook to offer a non-surveillance version might suggest that, while many users long for an surveilled internet, they’ve been taught that such a thing is not possible.
What does surveillance do to us?

What's the significance of pervasive surveillance on us as individuals and citizens? This is not a new topic. Thousands of commentators have reminded us that George Orwell's 1984 xxiv anticipated a society in which a government attempted to police thought by subjecting elite citizens to continual surveillance via telescreens, which both watched and recorded citizens behavior and broadcast images designed to combat thoughtcrime. While Orwell's imagery resonates well almost 70 years after it was authored, the analogy is inexact at best: Orwellian surveillance is visible, confrontational and deeply human - Winston Smith lives in constant fear of individuals who may be watching and waiting to inform on him. The surveillance Snowden helped reveal is invisible, secret and algorithmic. (It's also less targeted: one small consolation of surveillance in Orwell's Oceania is that it was targeted at educated elites, while the proletariat lived a life largely unobserved.)

Jeremy Bentham's design for the panopticon, as analyzed by Michel Foucault in Discipline and Punish xxv, is a more apt metaphor. Bentham's proposed prison design featured a central tower from which guards could look into any cell at any time. Foucault argues that Bentham's proposed design cannot be understood as purely architectural, but as part of a larger system of practices designed to transform prisoners into self-disciplining actors, a model as applicable to the factory as it was to the prison. As with prisoners watched via panopticon, internet users are not aware whether they are being watched at any given moment, or not, and that perpetual possibility of scrutiny likely shapes how we use this tool. Consider the invention of the "private mode" offered by most internet browsers - the implication is that the rest of our time online is anything but private, and that we'd need to choose to hide from scrutiny. (Of course, all the private mode does on most browsers is keeps sites from your browser history, helpful in avoiding scrutiny from your spouse or children, but not from advertisers tracking your movements online.)

If private browsing is a special mode, the default is public mode, an interesting inversion in that what we choose to read and watch has traditionally been a carefully protected aspect of personal privacy.

Two reasons the panopticon falls short as an analogy for surveillance after Snowden. One, the builders of the internet panopticon hadn't wanted to discipline those they were watching. Government surveillance becomes useless if it trains terrorists to act as if they're always being observed; commercial surveillance becomes less useful if we're aware that our online actions create a saleable profile, as we're more likely to take action to obscure or shape it. Second, the panopticon implies a single actor watching our behavior - subsequent scholars have suggested "the superpanopticon" or "the electronic panopticon" as broader terms. But the most helpful term for understanding how contemporary surveillance works is "the surveillant assemblage" xxvii, a term coined by Kevin Haggerty and Richard Ericson, building on the work of Gilles Deleuze and Felix Guattari.
The surveillant assemblage isn't a single system and isn't controlled by a single actor - it's what happens at the intersection of hundreds of commercial and government systems, and its power comes from collating and correlating these different pieces of information. Considering any form of surveillance in isolation gives an incomplete and inaccurate picture, as the ever-spreading, rhizomol nature of the assemblage means it's always incorporating new systems and new information.

The PRISM system, as explained in the documents released by Snowden, is a near-perfect exemplar of this rhizomol structure - systems that allowed corporations to monitor chat, email and other forms of communication became parts of the larger assemblage. It's here that the line between commercial and government surveillance blurs to the point of indistinguishability. Google had an incentive to store email as plaintext due to a commercial model where they support free email by algorithmically surveilling text and targeting ads based on keywords in user emails - when they came under pressure to share that information with the NSA, the systems architected to permit commercial surveillance were easily converted into the broader surveillant assemblage.

Avoiding the surveillant assemblage is impractical if not functionally impossible: "Privacy advocates bring this point home in their facetious advice that individuals who are intent on staying anonymous should not use credit, work vote or use the Internet." Add to that a prohibition on phone use and, given the rise of CCTV, a strict avoidance of public spaces and the challenge of following this advice becomes clearer. If the effect of big brother is to make you watch your speech carefully and plot revolution in a clandestine diary, and the effect of the panopticon is to turn you from a rebellious prisoner into a self-monitoring factory worker, the effect of the surveillant assemblage is to make you give up. Haggerty and Ericson call this "the disappearance of disappearance", the loss of the ability to be anonymous in public space.

The internet has a long and uncomfortable history with anonymity. Early internet boosters celebrated the idea that the internet’s anonymity would allow users to experiment with different identities, or to seek out information they might be uncomfortable searching for in the physical world - think of the gay teen in a small town looking for information and support. At the same time, we’ve blamed the internet’s often corrosive culture on anonymity and the idea that people behave badly online because anonymous actions are consequence free. Facebook’s insistence that people identify themselves by their real names online, and an attempt by Google to enforce similar rules on their Google+ social network, has led to a wave of online protest called Nymwars, but has also established real name identity as a norm for the majority of internet users. For long time users, the internet has never been a wholly anonymous and private space - as early as 1992, there have been cases on apparently anonymous online speech leading to real-world legal consequences. But for many of us, the possibility of searching for
information anonymously was a core internet value that has eroded in the face of Snowden's revelations.

Avoiding (Being Part of) Surveillance

Instead of asking if we can avoid being surveilled, we might ask the question, can we avoid becoming part of the surveillant assemblage. It’s a question we might ask of the newspapers responsible for publishing the Snowden revelations. Ghostery is a browser plugin that detects "web bugs", small pieces of code that detect when a user visits a website and transmits that information to web marketing firms that develop detailed user profiles that include information on the sites you visit - basically, when you're loading a webpage from a server you're also loading snippets of content from other servers all around the web - an ad on a webpage probably comes from a webserver run by an ad network. Some of these snippets are invisible - many webpages incorporate web bugs that help Google track how many people visit your webpage. Other bugs communicate information to third parties, aggregators and brokers of information. Uncomfortably, a good place to find some of these bugs is on the websites of The Guardian and the Washington Post, on the stories where they reveal NSA revelations.

Bob Sesca, who analyzed The Guardian’s use of web bugs on its surveillance coverage, writes at some length about a particular technology: Omniture, Adobe’s web analytics platform. Omniture has advertised that it is capable of collecting not only a user’s IP address, her hardware and software configuration and her usage of other sites that have the Omniture bug, but also her search history and behavior on social media. The presence of a web bug like Omniture’s on The Guardian's site is not an unwitting inclusion. These bugs take time to load and slow down page speed, which means that a sane webmaster would include them only because you’re paid to or because you have to. In Guardian’s case, their presence is likely because the publishers need detailed information on their readers to make their ads more saleable; allowing the presence of the Omniture bug on their site allows them to track where Guardian readers go after visiting the site, which becomes data they can sell to their advertisers.

There’s a distinction between tracking a user’s path through the internet and intercepting a person’s personal communications, and I don’t mean to construct a false equivalency. I also want to recognize that newspapers face a particularly fearsome problem when it comes to paying for their investigative reporting. Newspapers want to have a widespread civic impact, which means they want, if possible, to be accessible to as many readers as possible. Approaches to revenue that reduce reach - making content accessible only by paid subscription- reduce the reach and civic impact, which means that newspapers have a particular incentive to generate revenue through targeted ads.

That said, the similarities between the systems of surveillance that enable targeted advertising and those used by intelligence officials go beyond analogy; instead,
those systems have merged. An internal NSA slide presentation deck reveals that the NSA and GHQ use Google’s “PREF” cookie, used by Google to track preferences of users of their services, to identify an individual’s websurfing behavior in large sets of data. Google is so effective in identifying individual users in the crowd of the web that the NSA simply piggybacks on their technology. The NSA uses another Google cookie, set by the Doubleclick ad network, to “decloak” users who use Tor to disguise their IP address, determining that a Tor user with a given Doubleclick cookie is the same uncloaked user with the same cookie.xxx The very technologies used to deliver ads on newspaper stories about NSA surveillance are part of the NSA’s surveillance apparatus.

If we accept that newspapers have a civic responsibility beyond their commercial responsibility, we might ask whether The Guardian and The Post have a responsibility to help their readers understand commercial surveillance and its potentially corrosive effects. Given the pervasiveness of surveillance in our contemporary world, understanding surveillance should be a beat. We could imagine The Guardian publishing a user guide to safely reading the Guardian’s coverage of NSA surveillance as a form of public service. (I’ve included a brief version of such a guide as an addendum to this essay.)

**Surveillance free zones?**

In a world of pervasive surveillance, it’s both encouraging and strangely sad to see the emergence of spaces that are explicitly privacy respecting - the need for these spaces is almost as uncomfortable as the Orwellian "free speech zones" that have been built to accomodate the right to protest at public events. Libraries are probably the most visible of these privacy zones, as American librarians have been zealous defenders of the privacy rights of their patrons. Four Connecticut librarians fought a gag order associated with a national security letter demanding access to the logs of their internet-connected computers and have become some of the most visible opponents of these gag ordersxxx. The American Library Association now advises librarians on best policies for protecting user privacy, including destroying circulation records as soon as possible to keep them subpoena proofxxxii. The Massachusetts ACLU is working with local libraries to install Tor on their computers to provide patrons with a surveillance-resistant ability to access the internet.xxxiii

The emergence of libraries as surveillance-resistant spaces is important both in practical and symbolic terms. Even if we don’t feel the need to use a Tor-enabled browser to search for health information, the commitment librarians have made to protecting privacy, even when it’s expensive and inconvenient, is a reminder that civic responsibility can trump expediency. The existence of a surveillance-free space reminds us how rare these spaces are, and how much work is necessary to create and protect them.

The Guardian, The Washington Post and journalism as a whole should be proud of the important role they have played in prompting a national debate about...
surveillance, privacy and government overreach. But it is fair to ask whether these critical civic institutions, critical to ensure that we can take action as informed citizens, should find a way to escape their role as part of the surveillant assemblage and become another one of the rare, precious surveillance-resistant public spaces.

Addendum: On Safely Reading Newspaper Coverage of Surveillance

It is deeply ironic that reading coverage of NSA and GCHQ surveillance on The Washington Post and The Guardian websites subjects readers to surveillance by the newspapers, by advertising networks and, perhaps, by the NSA itself. It is possible to reduce the information shared with third parties while reading these stories, though technologies used to escape surveillance tend to lead to less rich user experiences on these sites. This brief guide suggests a number of methods, in order of increasing discomfort, that one could take to preserve one’s privacy while reading the fine surveillance coverage The Washington Post and The Guardian have produced.

- Don’t log on. Most newspapers offer customized content for subscribers, and readers tend to remain logged into these websites to avoid re-entering passwords when reading a website. This makes it very easy for a website to associate your personally identifiable subscriber information with your online behavior. Read these websites as a guest user, not one logged into the site.
- Block third party cookies. Even if you’re comfortable with a website knowing your reading behavior, you may not wish to share that behavior with the advertising companies the website has allowed to inject third-party cookies into the webpages you access. Apple’s Safari browser allows users to block third-party cookies explicitly (as well as blocking cookies entirely, which may lead to unpredictable behavior on sites that attempt to customize to your reading behavior.) Firefox users can use the Privacy Badger plugin to block third party cookies. Clear all cookies when you finish any web browsing session.
- Block ads. Even if you’re blocking third-party cookies, you are leaving traces in the logfiles of advertisers by loading ads from their webservers. AdBlock Plus is an effective and free tool for ad blocking.
- Don’t read using mobile devices. These devices are far harder to anonymize than web browsers on conventional computers, as mobile phones transmit a unique identifier to their networks when in use. This information is tracked by mobile internet service providers and is susceptible both towards subpoena requests and to NSA data aggregation. Furthermore, many mobile devices “leak” geolocation information to webservers. Ads are more valuable to advertisers if they can be targeted to a user’s location, so there is an incentive for developers of apps to leak this information.
- Use Tor. Even if you aren’t logged into a website and blocking cookies, you are identifying yourself through your IP address, which can sometimes be used to uniquely identify a computer and more often can be used to identify your rough geographic location. Tor routes your traffic through a set of intermediary computers using a clever scheme that makes it extremely
difficult for websites to know the actual IP address of your computer. (Even more cleverly, Tor knows that you're using the system, but not what sites you're visiting.) Using Tor will slow down your internet connection and using it in ways that successfully disguises your IP address requires you to turn off significant functionality in your web browser. (It is wise to turn off Javascript, which will likely break many features on most modern websites.) For those more concerned about security (this is probably overkill for reading a newspaper website safely), a portable operating system called Tails allows you to reboot a computer into a configuration that is highly secured and runs all communications through Tor.

- Use public computers. If your concern is ensuring that advertisers and publishers cannot connect your online behavior and your real-world identity, one solution is to use computers that cannot be traced to your identity. Many public libraries offer computers that allow you to access the internet without producing an ID. Your surfing behavior becomes indistinguishable from that of other users, so long as you avoid using services associated with your identity, like webmail, personalized search, etc.

- Read the physical newspaper, preferably purchased at a newsstand where you can make your purchase, in cash, out of the view of surveillance cameras.

---

i Applebaum, Jacob, “We Don’t Live In a Free Country”. Interview with Democracy Now!. Web, December 1, 2014: http://www.democracynow.org/2012/4/20/we_do_not_live_in_a_free_country


