**ERWC AOW 5 Period: Name:**

**Instructions**: Annotate the following using the S U C Q R process. Then add a one-page reflection to the article with your thoughts about what it says. If the reflection is hand-written, it must be a single-spaced page, taking into account the size of your handwriting. If it is typed, it must be Times New Roman, 12 point font, and double spaced.

# This Article Is Spying on You

*The New York Times*, By Timothy Libert, Sept. 18, 2019

The press has performed admirably in reporting on privacy violations by the National Security Agency and major internet companies. But news sites often expose users to the same surveillance programs and data-collection companies they criticize. Even articles that explained how the [N.S.A. was using Google cookies](https://www.washingtonpost.com/news/the-switch/wp/2013/12/10/nsa-uses-google-cookies-to-pinpoint-targets-for-hacking/?utm_term=.5c0ababaf46b) to “pinpoint targets for hacking” often included the exact same cookies revealed by Edward Snowden. Likewise, [articles about Facebook and Cambridge Analytica](https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election) often include Facebook tracking code, allowing Facebook to keep tabs on what people read.

Surveillance on news websites is particularly problematic because the news you consume may reveal your political leanings or health interests — information that is not just exploited by corporations to sell you things, but could also be abused by governments. And because news organizations benefit from the surveillance economy by running advertisements targeted to reader interests, they may be less likely to report on their own tracking practices.

A recent article by The Times headlined “[Can an Abortion Affect Your Fertility?](https://www.nytimes.com/2019/05/30/well/can-an-abortion-affect-your-fertility.html?module=inline)” provides a useful example of how privacy is infringed on by news websites. I used my software platform, [webXray](https://webxray.eu/), to load the article page 10 times in a row with the Chrome browser. During each page load the software kept track of data transfers made to outside companies and generated a summary of what happened. The analysis revealed that people reading the article online may be tracked by nearly 50 different companies, one of which is [Oracle BlueKai](https://www.oracle.com/marketingcloud/products/data-management-platform/). According to its website, BlueKai helps companies“[personalize](https://www.oracle.com/marketingcloud/products/data-management-platform/)”marketing campaigns by ingesting “[massive amounts](https://www.oracle.com/marketingcloud/products/data-management-platform/id-graph.html)” of data. The BlueKai privacy policy specifies users are categorized into “[health and wellness interest segments](https://www.oracle.com/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html)” which include open-ended categories such as “[health conditions](https://www.oracle.com/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html)” and “[medical terms](https://www.oracle.com/us/assets/health-wellness-data-segments-2537888.pdf).” Given that numerous companies may track users, this is only the tip of the iceberg.

There is a troubling lack of transparency in these practices. The [Times’s privacy policy](https://help.nytimes.com/hc/en-us/articles/115014892108-Privacy-policy) does not disclose the vast majority of tracking companies (including BlueKai) on its site, requires users to accept cookies to fully use the site and explicitly states that The Times ignores the “do not track” browser setting. This type of tracking is standard practice in the news industry, and The Times is far from the worst offender.

In a [recent study I conducted with Reuben Binns](https://timlibert.me/pdf/LIBERT_BINNS-2019-GOOD_NEWS.pdf), we compared 4,000 United States-based news sites with 4,000 non-news sites. The news sites exhibited a significantly higher reliance on outside companies to manage a range of site functions such as advertising and hosting fonts. These outside companies often maintain vast databases of personal web browsing habits, which they may sell or use for targeting advertisements.

Some of these companies, like Google and Facebook, [have cooperated with the N.S.A](https://www.nytimes.com/2013/06/08/technology/tech-companies-bristling-concede-to-government-surveillance-efforts.html?module=inline). and may be legally required to disclose user data to law enforcement. Some may do so voluntarily. Worse, only 10 percent of these outside parties are disclosed in privacy policies of the news sites we studied, meaning even diligent readers will never learn who collects their data. From a privacy perspective, news websites are among the worst on the web.

News organizations did not create the surveillance-for-profit system that exists today. At the dawn of the internet era, advertisers demanded tracking to ensure that ads were being shown to humans, not bots. Then, as advertisers pushed for ways to better target ads, ad tech companies created vast networks to harvest user data and broker ads on billions of web pages, At the same time that ad tech networks began to dominate web advertising, traditional forms of advertising and subscription revenue for newspapers began to dry up. In a rush to stop the bleeding, many news outlets partnered with ad tech companies to gain entry to their expanding networks. These early decisions put news organizations on a path whereby they sacrificed reader privacy, reduced their ability to maintain direct relationships with advertisers and ultimately put their survival in the hands of middlemen like Google.

The result is that as online advertising networks become more highly centralized, the old model of a independently managed and free press is being replaced by one where giant technology companies control user data and the purse strins. While the problems are significant, two approaches, both mandated by Europe’s General Data Protection Regulation, or G.D.P.R., might benefit news outlets and readers. The first, [data protection impact assessments](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679#d1e3546-1-1), requires organizations to engage with users so their needs may be understood and considered. This could involve creating a digital ombudsman or public editor to represent the privacy concerns of readers.

A second G.D.P.R.-mandated approach, [privacy by design](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679#d1e3063-1-1), requires tech companies to develop software that makes privacy the default mode of operation, embedded at all levels of a system. In privacy by design, respect for users is paramount. Instead of tracking users as the default, requiring them to “opt-out,” the default in privacy-by-design is that users must “opt in” to tracking used for advertising. The result may be less precisely targeted advertising — and much greater privacy.

Like any piece of large legislation, [G.D.P.R. is complicated](https://www.nytimes.com/2018/05/15/opinion/gdpr-europe-data-protection.html?module=inline). But improving user privacy can be quite simple. When I loaded “[Can an Abortion Affect Your Fertility?](https://www.nytimes.com/2019/05/30/well/can-an-abortion-affect-your-fertility.html?module=inline)” in the European Union, I discovered that The Times has a cookie called “nyt-gdpr.**”** When readers load an article on the Times website, those protected by G.D.P.R. get a page that better protects their privacy. In comparison to the nearly 50 companies tracking users on that article in the United States, I found only 16 in the European Union. On the United States version of the Times website, I also found over 100 cookies placed by outside companies, compared to just 28 in Europe.

Jean-Christophe Demarta, an advertising executive at The Times, recently told Digiday that even with G.D.P.R.-related changes, The Times’s “[digital advertising business continues to grow nicely](https://digiday.com/media/gumgumtest-new-york-times-gdpr-cut-off-ad-exchanges-europe-ad-revenue/).” If people everywhere should have the same fundamental rights to privacy as Europeans, and if providing privacy is not unduly harming revenue, why shouldn’t The Times provide enhanced privacy to all its readers? Readers everywhere could then be more confident that their interests in politics, health and other sensitive topics would not be subject to government surveillance or sold to the highest bidder. In the same way The Times leads in high-quality news coverage, it could also lead in respecting reader privacy.

Timothy Libert is a faculty member in computer science at Carnegie Mellon University, where he teaches in the [privacy engineering program](https://privacy.cs.cmu.edu/index.html).

Like other media companies, The Times collects data on its visitors when they read stories like this one. For more detail please see [our privacy policy](https://help.nytimes.com/hc/en-us/articles/115014892108-Privacy-policy?module=inline) and [our publisher's description](https://www.nytimes.com/2019/04/10/opinion/sulzberger-new-york-times-privacy.html?rref=collection%2Fspotlightcollection%2Fprivacy-project-does-privacy-matter&action=click&contentCollection=opinion&region=stream&module=inline&version=latest&contentPlacement=8&pgtype=collection) of The Times's practices and continued steps to increase transparency and protections.

**Reflection instructions**: Using your annotations, write a one-page reflection on the points made within the article. This is not a formal essay, but be sure to reflect on and refer to the contents of the article, whether positively or otherwise.