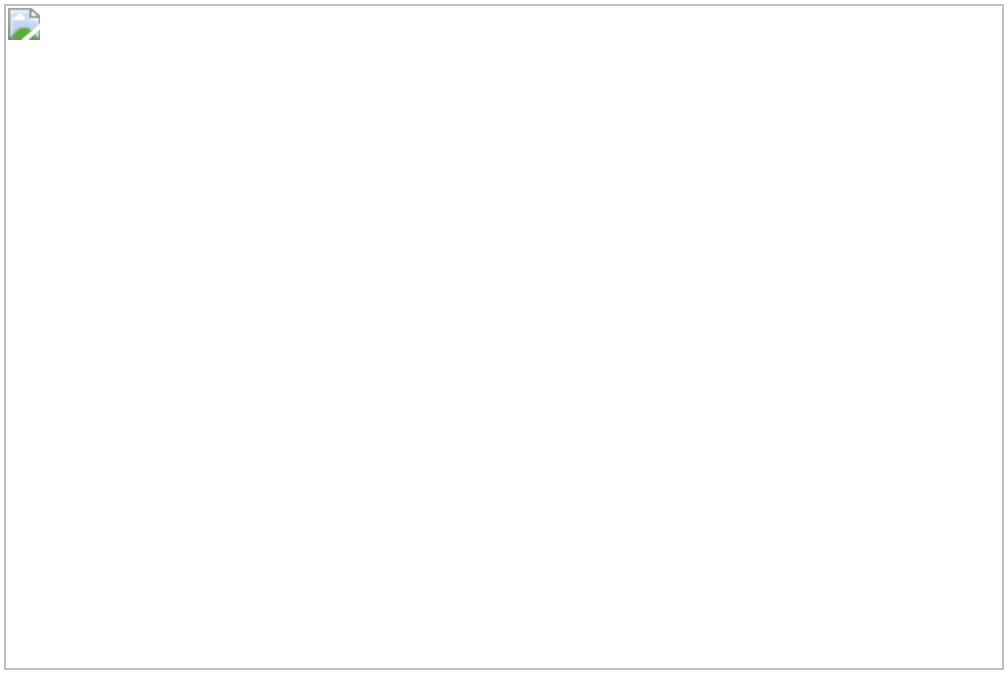
Everyone Has Got A Surveillance Spy Score And It Can Cost You Big Money

Profile picture for user Tyler Durden
by Tyler Durden

Authored by Dagny Taggart

In these Orwellian times, when it is revealed that yet another government agency is spying on us in yet another way, most of us aren't one bit surprised. **Being surveilled nearly everywhere we go (and even in our own homes) has become the norm**, unfortunately.



Yesterday, it was revealed that the NSA improperly collected Americans' call and text logs in November 2017 and in February and October 2018 – just months after the agency claimed it was going to delete the 620 million-plus call detail records it already had stockpiled.

But this article isn't about that.

It is about something far more insidious.

When it comes to spying on people, the government has competition.

The Chinese government is currently implementing a social credit system to monitor its 1.3 billion citizens (China already has 200 million public surveillance cameras). Facial recognition technology and personal data from cell phones and digital transactions are being used to collect intimate details about people's lives, including their purchasing habits and whom they socialize with.

The gathered data is used to create mandatory social credit ratings for every citizen. These ratings will score citizens' "general worthiness" and provide those with higher scores opportunities like access to jobs, loans, and travel. Those with lower scores will not have access to those opportunities.

While the United States government has yet to implement such a system, *companies* in the country are, reports The Hill:

> Consumer advocates are pushing regulators to investigate what they paint as a shadowy online practice where retailers use consumer information collected by data brokers to decide how much to charge individual customers or the quality of service they'll offer.
>
> #REPRESENT, a public interest group run by the Consumer Education Foundation in California, filed a complaint with the Federal Trade Commission (FTC) on Monday asking the agency to investigate what the group is calling "surveillance

scoring” of customers’ financial status or creditworthiness. (source)

Companies are using Secret Surveillance Scores to evaluate you.

The opening paragraphs of the 38-page complaint are chilling:

> Major American corporations, including online and retail businesses, employers and landlords are using Secret Surveillance Scores to charge some people higher prices for the same product than others, to provide some people with better customer services than others, to deny some consumers the right to purchase services or buy or return products while allowing others to do so and even to deny people housing and jobs.
>
> The Secret Surveillance Scores are generated by a shadowy group of privacy-busting firms that operate in dark recesses of the American marketplace. They collect thousands or even tens of thousands of intimate details of each person's life – enough information, it is thought, to literally predetermine a person's behavior – either directly or through data brokers. Then, in what is euphemistically referred to as "data analytics," the firms' engineers write software algorithms that instruct computers to parse a person's data trail and develop a digital "mug shot." Eventually, that individual profile is reduced to a number – the score – and transmitted to corporate clients looking for ways to take advantage of, or even avoid, the consumer. The scoring system is automatic and instantaneous. None of this is disclosed to the consumer: the existence of the algorithm, the application of the Surveillance Score or even that they have become the victim of a technological scheme that just

a few years ago would appear only in a dystopian science fiction novel. (source)

These scores are used to discriminate based on income.

Written by lawyers Laura Antonini, the policy director of the Consumer Education Foundation, and Harvey Rosenfield, who leads the foundation, the complaint highlights four areas in which companies are using surveillance scoring: pricing, customer service, fraud prevention, and housing and employment.

> "This is a way for companies to discriminate against users based on income and wealth," Antonini told The Hill.
>
> "It can range from monetary harm or basic necessities of life that you're not getting."

Antonini and Rosenfield argue that the practices outlined in the complaint are illegal – and that consumers are largely unaware that they're being secretly evaluated in ways that can influence how much they pay online.

"The ability of corporations to target, manipulate and discriminate against Americans is unprecedented and inconsistent with the principles of competition and free markets," the complaint reads. "Surveillance scoring promotes inequality by empowering companies to decide which consumers they want to do business with and on what terms, weeding out the people who they deem less valuable. Such discrimination is as much a threat to democracy as it is to a free market."

Stores are using this scoring system to charge you higher prices.

Here's more detail, from The Hill:

> The filing points to a 2014 Northeastern University study exploring the ways that companies like Home Depot and Walmart use consumer data to customize prices for different customers. Rosenfield and Antonini replicated the study using an online tool that compares prices that they're charged on their own computers with their own data profiles versus the prices charged to a user browsing sites through an anonymized computer server with no data history.
>
> What they found was that Walmart and Home Depot were offering lower prices on a number of products to the anonymous computer. In the search results for "white paint" on Home Depot's website, Rosenfield and Antonini were seeing higher prices for six of the first 24 items that popped up.
>
> In one example, a five-gallon tub of Glidden premium exterior paint would have cost them $119 compared with $101 for the anonymous computer.
>
> A similar pattern emerged on Walmart's website. The two lawyers found the site was charging them more on a variety of items compared with the anonymous web tool, including paper towels, highlighters, pens and paint.
>
> One paper towel holder cost $10 less for the blank web user. (source)

To see screenshots of different “personalized” prices shown for items from Home Depot and Walmart, please see pages 12-16 of the complaint. The examples presented demonstrate just how much these inflated prices for common household goods can really add up.

The travel industry is particularly sneaky.

A few days ago, we reported on hidden fees that could be costing you big bucks. The travel industry is a particularly large offender when it comes to sneaky fees, and they are also implicated in this scheme:

Travelocity. Software developer Christian Bennefeld, founder of etracker.com and eBlocker.com, did a sample search for hotel rooms in Paris on Travelocity in 2017 using his eBlocker device, which "allows him to act as if he were searching from two different" computers. Bennefeld found that when he performed the two searches at the same time, there was a $23 difference in Travelocity's prices for the Hotel Le Six in Paris.

CheapTickets. The Northeastern Price Discrimination Study found that the online bargain travel site CheapTickets offers reduced prices on hotels to consumers who are logged into an account with CheapTickets, compared to those who proceed as "guests." We performed our own search of airfares on CheapTickets without being logged in. We searched for flights from LAX to Las Vegas for April 5 through April 8, 2019. Our searches produced identical flight results in the same order, but Mr. Rosenfield's prices were all quoted at three dollars higher than Ms. Antonini's.

Other travel websites. The Northeastern Price Discrimination Study found that Orbitz also offers reduced prices on hotels to consumers who were logged into an account (Orbitz has been accused of quoting higher prices

to Mac users versus PC users because Mac users have a higher household income); Expedia and Hotels.com steer a subset of users toward more expensive hotels; and Priceline acknowledges it “personalizes search results based on a user’s history of clicks and purchases. (source)

There is an industry that exists to evaluate you and sell your data to companies.

The complaint also describes an industry that offers retailers evaluations of their customers' "trustworthiness" to determine whether they are a potential risk for fraudulent returns. One such firm – called Sift – offers these evaluations to major companies like Starbucks and Airbnb. Sift boasts on its website that it can tailor "user experiences based on 16,000+ real-time signals – putting good customers in the express lane and stopping bad customers from reaching the checkout."

The Hill contacted Sift for comment, and the company was not able to respond. But, back in April, a Sift spokesperson told The Wall Street Journal that it rates customers on a scale of 0 to 100, likening it to a credit score for trustworthiness.

While credit scores can wreak havoc on a person's ability to make big purchases (and sometimes, gain employment), they at least are transparent. Surveillance scoring is not. There is NO transparency for consumers, and Rosenfield and Antonini argue that companies are using them to engage in illegal discrimination while users have little recourse to correct false information about them or challenge their ratings.

We are being spied on and scored on a wide variety of factors.

“In the World Privacy Forum’s landmark study “The Scoring of America: How Secret Consumer Scores Threaten Your Privacy and Future,” authors Pam Dixon and Bob Gellman identified approximately 44 scores currently used to predict the actions of consumers,” the complaint explains:

> These include:
>
> The Medication Adherence Score, which predicts whether a consumer is likely to follow a medication regimen;
>
> The Health Risk Score, which predicts how much a specific patient will cost an insurance company;
>
> The Consumer Profitability Score, which predicts which households may be profitable for a company and hence desirable customers;
>
> The Job Security score, which predicts a person’s future income and ability to pay for things;
>
> The Churn Score, which predicts whether a consumer is likely to move her business to another company;
>
> The Discretionary Spending Index, which scores how much extra cash a particular consumer might be able to spend on non-necessities;

The Invitation to Apply Score, which predicts how likely a consumer is to respond to a sales offer;

The Charitable Donor Score, which predicts how likely a household is to make significant charitable donations;

The Pregnancy Predictor Score, which predicts the likelihood of someone getting pregnant. (source)

The government isn't doing anything to stop these practices.

Back in 2014, the Federal Trade Commission held a workshop on a practice they call "predictive scoring" but the agency has done little since to reign in the practice. Antonini said that their complaint is pushing the agency to reexamine the industry and investigate whether it violates laws against unfair and deceptive business practices, according to The Hill:

> **"It's far, far worse than when they looked at it in 2014,"** she said. "There's an exponentially larger amount of data that's being collected about the American public that's in the hands of data brokers and companies. **Their ability to process that data and write algorithms have also improved exponentially.**" (source)

We seem to be past the point of expecting our data to remain private, The Introduction to the complaint begins with a passage that sums up reality for us now:

> This Petition does not ask the Commission to investigate the collection of Americans' personal information. The battle over whether Americans' personal data can be collected is over, and, as of this moment at least, consumers have lost. Consumers are now victims of an unavoidable corporate surveillance capitalism.
>
> Rather, this Petition highlights a disturbing evolution in how consumers' data is deployed against them. (source)

We can’t go anywhere without being surveilled now.

It is now impossible to shop in any large chain stores without being spied on. Stores are starting to use “smart coolers”, which are refrigerators equipped with cameras that scan shoppers’ faces and make inferences on their age and gender. And, a recent article from Futurism describes how security cameras are no longer being used solely to reduce theft:

> “Instead of just keeping track of who’s in a store, surveillance systems could use facial recognition to determine peoples’ identities and gathering even more information about them. That data would then be out there, with no opportunity to opt out. (source)

A new ACLU report titled “The Dawn of Robot Surveillance” describes how emerging AI technology enables security companies to constantly monitor and collect data about people.

> ***“Growth in the use and effectiveness of artificial intelligence techniques has been so rapid that people haven’t had time to assimilate a new understanding of what is being done, and what the consequences of data collection and privacy invasions can be,”*** the report concludes.