MERCOLA
Take Control of Your Health

Will Google's Social Credit System Determine Your Future?

Analysis by Dr. Joseph Mercola – Expert Review by
Maryam Henein ✔ Fact Checked

February 14, 2023

STORY AT-A-GLANCE

- China started rolling out a social credit system in 2018, which awards and subtracts points for certain types of behavior
- Google is the largest monopoly the world has ever seen, and its data-siphoning tentacles reach deep into our everyday lives, collecting data on every move you make and conversation you have, whether online or in the real world
- By the end of 2021, approximately 1 billion cameras will be watching public movements across the globe. Cities are also inviting residents and businesses to plug their private surveillance cameras into their police network, which expands the surveillance system even further
- To make sense of all this footage, video analytic software and artificial intelligence are used. Video analytic capabilities include fight and fall detection, loitering and motion recognition, dog walking, jaywalking, toll fare evasion and lie detection
- There are now proposals suggesting all of this data, in combination with AI-enabled analytics systems, could be used for "predictive policing" as illustrated in the 2002 movie "Minority Report," where suspected perpetrators are arrested before actually committing the crime

You may have heard about China's social credit system — a dystopian monitoring scheme focused on the moral dimension of human life and behavior — which was

conceived in 2014 and rolled out in in earnest in 2018. As reported by Business Insider in October that year:[1]

> *"Like private credit scores, a person's social score can move up and down depending on their behavior. The exact methodology is a secret — but examples of infractions include bad driving, smoking in non-smoking zones, buying too many video games and posting fake news online.*
>
> *China has already started punishing people by restricting their travel. Nine million people with low scores have been blocked from buying tickets for domestic flights ...*
>
> *They can also clamp down on luxury options — three million people are barred from getting business-class train tickets. The eventual system will punish bad passengers specifically. Potential misdeeds include trying to ride with no ticket, loitering in front of boarding gates, or smoking in no-smoking areas."*

Aside from impeding your ability to travel, an individual's punishment for "bad behavior" per the social credit system can also result in slower internet speed, being banned from attending certain schools or getting a higher education, being barred from certain types of employment, confiscation of pets and, of course, public shaming.[2]

Google Makes Orwellian Surveillance Easy

In the bitchute video above, Truthstream Media details how this kind of public "trustworthiness" scoring can alter the way people behave — indeed their view of reality itself, and the vast data mining required for the system to work. As noted in the video:

> *"Social credit scores award or remove points based on behavior. It's Big Data meets Big Brother. This will be a world with no more personal experiences, only transactions for the social credit system.*
>
> *This [the system] knows every person, every bike, every car, every bus. That's because it essentially turns every public interaction into a transaction where*

points can be earned or lost."

Google, of course, is a perfect fit for this kind of Orwellian surveillance scheme. It is, by far, the largest monopoly the world has ever seen, and its data-siphoning tentacles reach deep into our everyday lives, collecting data on every move you make and conversation you have, whether online or in the real world.

Google actually tracks your movements online, even when you don't think you are using their products. Most websites you visit use the 'free' Google Analytics program to track everything you do on a website. Google purchased Urchin Software back in 2005, and by giving it away were able to integrate this important surveillance tool into most of the internet.

Google Analytics integrates with Google's ad network monopoly, as well as the largest email service Gmail. These systems are not free, they are a tightly integrated package of surveillance tools - selling your data, selling ads served to you, and manipulating content to direct your behavior.

These tools collect data along with other Google products like the Android 'smart' phones, the Nest home security system, and even Google's Home Assistant. You can expect these surveillance products to become free over time as the absolute goal is to exploit every bit of data they can collect from you.

A 2015 Wired article[3] revealed some of the details of how Google's online empire is built, noting "One of the company's cluster switches provides about 40 terabits per second of bandwidth — the equivalent of 40 million home internet connections," and "Google now sends more information between its data centers than it trades with the internet as a whole."

As highlighted in a January 27, 2020, article[4] by The Intercept, smart camera networks equipped with facial recognition and video analytic software will advance global surveillance even further, and should be banned to prevent an inevitable slide into invisible yet all-encompassing authoritarianism.

> *"The rise of all-seeing smart camera networks is an alarming development that threatens civil rights and liberties throughout the world.*
>
> *Law enforcement agencies have a long history of using surveillance against marginalized communities, and studies show surveillance chills freedom of expression — ill effects that could spread as camera networks grow larger and more sophisticated,"* The Intercept notes.[5]

Silicon Valley Is Building America's Social Credit System

According to Fast Company,[6] China's social credit system is not entirely unique. "A parallel system is developing in the United States, in part as the result of Silicon Valley and technology-industry user policies, and in part by surveillance of social media activity by private companies," Fast Company writes.[7]

For example, life insurance companies can now use content shared in social media posts to determine your premium. "That Instagram pic showing you teasing a grizzly bear at Yellowstone with a martini in one hand, a bucket of cheese fries in the other, and a cigarette in your mouth, could cost you," Fast Company notes.[8]

PatronScan is another example. These devices are used by restaurants to identify fake IDs and undesirable customers — people previously removed from an establishment for causing a fight, committing sexual assault, stealing or doing drugs.

The list is shared among PatronScan customers, so getting banned in one bar or restaurant effectively bans you from all bars and restaurants in the U.S., Canada and U.K. for up to one year. For additional examples, see the original Fast Company article.[9]

The Expansion of Public Video Surveillance

Many TV's now have a camera and can be used to **record your emotions** while watching presidential debates or the evening news. The Intercept article[10] cited earlier goes on to detail the rise and expansion of video surveillance, starting with Axis Communications'

internet-enabled surveillance camera, launched in the late '90s, to more modern video management systems that organize all this visual data into databases.

By the end of 2021, the marketing firm IHS Markit predicts 1 billion cameras will be watching public movements across the globe. As if that's not enough, cities are also inviting residents and businesses to plug their private surveillance cameras into their police network, which expands the system even further.

According to The Intercept, Detroit, Chicago, New Orleans, New York City and Atlanta have all deployed these types of "plug-in surveillance networks," and many others are considering it as well. To actually make sense of all this footage, video analytic software and artificial intelligence (AI) are used.

Video analytic capabilities include "fight detection, motion recognition, fall detection, loitering, dog walking, jaywalking, toll fare evasion and even lie detection," The Intercept reports.[11]

Object recognition and "anomalous or unusual behavior detection" are also used to flag particular incidents that are then reviewed by human eyes. The Intercept recounts how this information can be used by law enforcement to identify potential crime situations:

> *"In Connecticut, police have used video analytics to identify or monitor known or suspected drug dealers.*
>
> *Sergeant Johnmichael O'Hare, former Director of the Hartford Real-Time Crime Center, recently demonstrated how BriefCam helped Hartford police reveal 'where people go the most' in the space of 24 hours by viewing footage condensed and summarized in just nine minutes.*
>
> *Using a feature called 'pathways,' he discovered hundreds of people visiting just two houses on the street and secured a search warrant to verify that they were drug houses."*

Is a 'Pre-Crime' Department Next?

Companies are also working on searchable databases that can access and make sense of visual data from a range of different platforms, which will "supercharge the ability to search and surveil public spaces," The Intercept says.[12]

What's more, there are now proposals suggesting all of this data, in combination with AI-enabled analytics systems, could be used for "predictive policing" as illustrated in the 2002 movie "Minority Report," where suspected perpetrators are arrested before actually committing the crime.

Sound too crazy to be true? The Intercept cites a 2018 document[13] by the data storage firm Western Digital and the consulting company Accenture, "Value of Data: Seeing What Matters — A New Paradigm for Public Safety Powered by Responsible AI," which predicts smart surveillance networks may be deployed "across three tiers of maturity."

The first tier is where we're at now, where law enforcement use CCTV networks to investigate crimes after they've already occurred.

At the second tier level, predicted to be in place by 2025, municipalities will be transformed into fully connected "smart cities," where the cameras of businesses and public institutions are all plugged into a government-run AI-enabled analytics system. The third tier, predicted by 2035, will have predictive capabilities. As reported by The Intercept:[14]

> *"A 'public safety ecosystem' will centralize data 'pulled from disparate databases such as social media, driver's licenses, police databases, and dark data.' An AI-enabled analytics unit will let police assess 'anomalies in real time and interrupt a crime before it is committed.' That is to say, to catch pre-crime."*

Google's Ad Network Monopoly

Google's monopoly goes well beyond web search. It also has a potentially dangerous monopoly on online advertising. In 2007, Google bought DoubleClick, which already dominated the digital advertising market. As reported by InfoWorld:[15]

> *"Here's the danger: Google already knows a tremendous amount about the traffic it sends to individual Web sites — where it comes from, what people are looking for, even some basic demographics.*
>
> *With DoubleClick in the fold, they will also know what ads are being served on any given page. That gives Google unprecedented insight into publishers' business. And remember, those publishers may be partners, but they are also competitors, often trying to woo the same advertisers as Google.*
>
> *Web sites live and die based upon ad revenue and on charging advertisers a certain rate based upon the number of pages served and the quality of their readership/user base. I could imagine a not-entirely-paranoid fantasy in which Google can run the numbers, turn around, and offer better rates to advertisers for a similar audience."*

To learn more of Google's surveillance of you and those you love, please view my comprehensive interview with Robert Epstein below. Epstein, former editor-in-chief at Psychology Today, is now a senior research psychologist for the American Institute of Behavioral Research and Technology, where for the last decade he has helped expose **Google's manipulative and deceptive practices**.

Google Goes After Your Health Data

More recently, it's also become apparent Google is going after everyone's health data. Fitbit, which was recently purchased by Google, will provide them with all your physiological information and activity levels, in addition to everything else that Google already has on you.

As discussed in "How Google Is Stealing Your Personal Health Data," Google, Amazon and Microsoft also collect data entered into health and diagnostic sites, which is then shared with hundreds of third parties — and this data is not anonymized, meaning it's tied specifically to you, without your knowledge or consent.

In other words, DoubleClick, Google's ad service, will know which prescriptions you've searched for on Drugs.com, for example, thus providing you with personalized drug ads. "There is a whole system that will seek to take advantage of you because you're in a compromised state," Tim Libert, a computer scientist at Carnegie Mellon University told Financial Times.[16]

Google and various tech startups have even been investigating the possibility of assessing mental health problems using a combination of electronic medical records and tracking your internet and social media use.

Undisclosed data mining is also occurring in hospitals. A whistleblower recently revealed Google amassed health data from millions of Americans in 21 states through its Project Nightingale, and patients have not been informed of this data mining.[17,18] As reported by The Guardian:[19]

> *"The secret scheme ... involves the transfer to Google of healthcare data held by Ascension, the second-largest healthcare provider in the U.S. The data is being transferred with full personal details including name and medical history and can be accessed by Google staff. Unlike other similar efforts it has not been made anonymous though a process of removing personal information known as de-identification ..."*

According to Google and Ascension, the data being shared will be used to build a search tool with machine-learning algorithms that will spit out diagnostic recommendations and suggestions for medications that health professionals can then use to guide them in their treatment.

Google claims only a limited number of individuals will have access to the data, but just how trustworthy is Google these days? Since the data includes full personal details, sooner or later, they're likely to find a way to use it.

Google and Mastercard Track Your Purchasing Habits

Your credit card data, which at first glance would appear completely separate from Google, is also being used by the internet giant to customize ads. As reported by Bloomberg[20] August 31, 2018, four unnamed insiders, three of whom claim to have been directly involved in the negotiations, claim Google and Mastercard brokered a business alliance that gives Google access to Mastercard users' retail spending.

The two companies never made the agreement public, though. Christine Bannan, counsel with the advocacy group Electronic Privacy Information Center (EPIC) told Bloomberg:[21]

> *"People don't expect what they buy physically in a store to be linked to what they are buying online. There's just far too much burden that companies place on consumers and not enough responsibility being taken by companies to inform users what they're doing and what rights they have."*

According to Google, Mastercard users can opt out of ad tracking using Google's online Web & App Activity console.[22] The question is, how would users know to do that when they were never told such tracking was occurring in the first place?

Google's Store Sales Measurement service also suggests it's not just Mastercard users that are being tracked. As noted by Bloomberg, when Google announced the new sales measurement service in 2017, it claimed it had access to about 70% of U.S. credit and debit card sales.

Goodbye Google

To have any chance of protecting your privacy, you simply must avoid Google products, as they account for the greatest personal data leaks in your life. To that end, Mercola.com is now Google-free. We do not use Google Analytics, Google ads or Google search for internal searches. To boycott Google, be sure to ditch or replace:

- **Gmail**, as every email you write is permanently stored. It becomes part of your profile and is used to build digital models of you, which allows them to make predictions about your line of thinking and every want and desire.

Many other older email systems such as AOL and Yahoo are also being used as surveillance platforms in the same way as Gmail. ProtonMail.com, which uses end-to-end encryption, is a great alternative and the basic account is free.

- **Google's Chrome browser**, as everything you do on there is surveilled, including keystrokes and every webpage you've ever visited. Brave is a great alternative that takes privacy seriously.

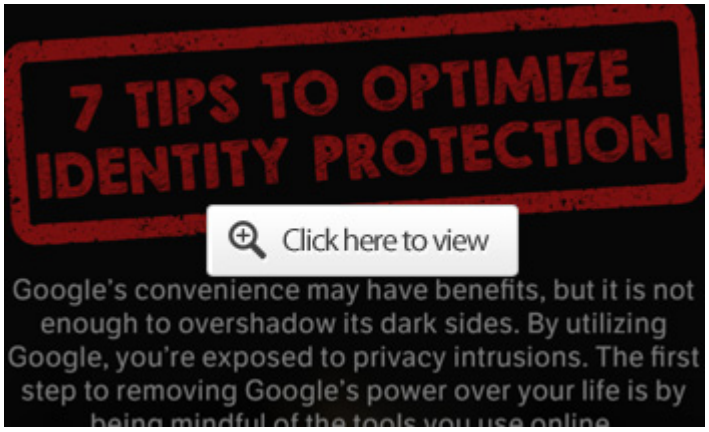
  Brave is also faster than Chrome, and suppresses ads. It's based on Chromium, the same software code that Chrome is based on, so you can easily transfer your extensions, favorites and bookmarks.

- **Google search engine, or any extension of Google**, such as Bing or Yahoo, both of which draw search results from Google. The same goes for the iPhone's personal assistant Siri, which draws all of its answers from Google.

  Alternative search engines include SwissCows and Qwant. Avoid StartPage, as it was recently bought by an aggressive online marketing company, which, like Google, depends on surveillance.

- **Android cellphones**, which run on a Google-owned operating system, can track you even when you're not connected to the internet, whether you have geo tracking enabled or not. Blackberry is more secure than Android phones or the iPhone. Blackberry's upcoming model, the Key3, may be one of the most secure cellphones in the world.

- **Google Home devices**, as they record everything that occurs in your home or office, both speech and sounds such as brushing your teeth and boiling water, even when they appear to be inactive, and send that information back to Google. Android phones are also always listening and recording, as are Google's home thermostat Nest, and Amazon's Alexa.



Additional Privacy Tips

In my recent interview (above) with Epstein, he also offered the following guidance for those seeking to protect their online privacy:

- **Use a virtual private network (VPN) such as Nord,** which is only about $3 per month and can be used on up to six devices. In my view, this is a must if you seek to preserve your privacy. Epstein explains:

  > *"When you use your mobile phone, laptop or desktop in the usual way, your identity is very easy for Google and other companies to see. They can see it via your IP address, but more and more, there are much more sophisticated ways now that they know it's you. One is called browser fingerprinting.*
  >
  > *This is something that is so disturbing. Basically, the kind of browser you have and the way you use your browser is like a fingerprint. You use your browser in a unique way, and just by he way you type, these companies now can instantly identify you.*
  >
  > *Brave has some protection against a browser fingerprinting, but you really need to be using a VPN. What a VPN does is it routes whatever you're doing through some other computer somewhere else. It can be anywhere in the world, and there are hundreds of companies offering VPN services. The one I like the best right now is called Nord VPN.*

You download the software, install it, just like you install any software. It's incredibly easy to use. You do not have to be a techie to use Nord, and it shows you a map of the world and you basically just click on a country.

The VPN basically makes it appear as though your computer is not your computer. It basically creates a kind of fake identity for you, and that's a good thing. Now, very often I will go through Nord's computers in the United States. Sometimes you have to do that, or you can't get certain things done. PayPal doesn't like you to be in a foreign country for example."

Nord, when used on your cellphone, will also mask your identity when using apps like Google Maps.

- **Clear your cache and cookies —** As Epstein explains in his article:[23]

  "Companies and hackers of all sorts are constantly installing invasive computer code on your computers and mobile devices, mainly to keep an eye on you but sometimes for more nefarious purposes.

  On a mobile device, you can clear out most of this garbage by going to the settings menu of your browser, selecting the 'privacy and security' option and then clicking on the icon that clears your cache and cookies.

  With most laptop and desktop browsers, holding down three keys simultaneously — CTRL, SHIFT and DEL — takes you directly to the relevant menu; I use this technique multiple times a day without even thinking about it. You can also configure the Brave and Firefox browsers to erase your cache and cookies automatically every time you close your browser."

- **Don't use Fitbit**, as it was recently purchased by Google and will provide them with all your physiological information and activity levels, in addition to everything else that Google already has on you.

Sources and References

- [1, 2] Business Insider October 29, 2018
- [3] Wired June 17, 2015
- [4, 5, 10, 11, 12, 14] The Intercept January 27, 2020
- [6, 7, 8, 9] Fast Company August 26, 2019
- [13] Western Digital, Accenture, Value of Data: Seeing What Matters — A New Paradigm for Public Safety Powered by Responsible AI (PDF)
- [15] InfoWorld April 13, 2007
- [16] Financial Times November 12, 2019
- [17] Financial Times November 14, 2019
- [18] Wall Street Journal November 11, 2019
- [19] The Guardian November 12, 2019
- [20, 21, 22] Bloomberg Updated August 31, 2018 (Archived)
- [23] Medium March 17, 2017