OneRep

WHITEPAPER

THE CONSUMER PRIVACY OUTLOOK FOR 2021: 7 NOTABLE TRENDS

Key factors that affect U.S. consumer data vulnerability and how they drive business and consumer action.

2021

Introduction

The pandemic has accelerated our use of digital tools and dependence on the online environment. With such huge increases in digital use come increased vulnerabilities to consumer privacy. While legislators slowly gain ground towards understanding the new digital environment, consumers are waking up to realizations that they need to get proactive in protecting their privacy.

Here are the important considerations in 2021.

1 The Internet of Things will continue affecting privacy

The ubiquity of the Internet of Things (IoT) makes consumer privacy increasingly difficult.

The amount of data being collected grows exponentially

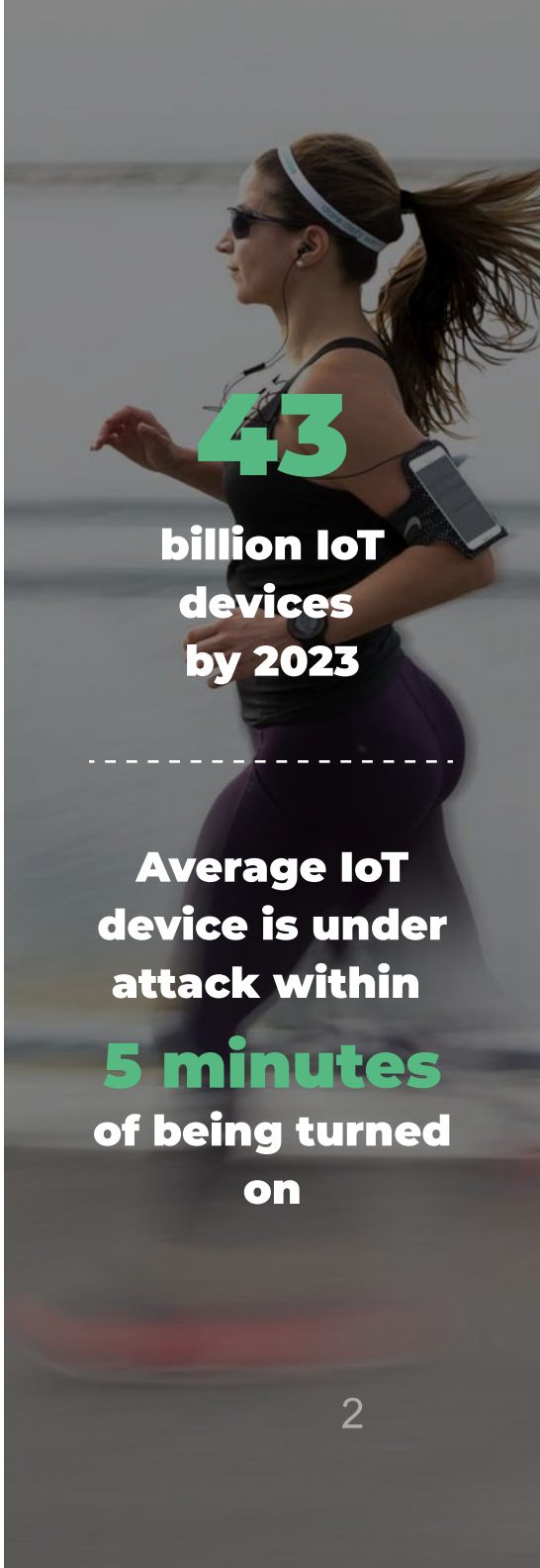
The number of IoT-connected devices is projected to increase to 43 billion by 2023. This will lead to an unprecedented accumulation of consumer data.

Increasing sensitivity of the collected data

People invite connected devices into their homes or on and into their bodies. Trackers, smart jewelry, wearable medical devices—all send data to health and fitness apps, many of which share that data with Facebook in order to reach existing and new users on the platform through ads. Amazon Alexa has long been accused of spying on its users. But not all smart home devices need a microphone to listen to you. This research showed that it is possible to exploit a robot vacuum cleaner to eavesdrop on homeowners' private conversations.

Vulnerability to hacking

Once a device is activated, manufacturers and hackers can use it to virtually invade our homes and our bodies. The opportunities for such an invasion will continue to grow exponentially. Each connected device creates thousands of discrete entry points for hackers, leaving sensitive information vulnerable. Notable fact: An average IoT device is targeted by a cyber attack within as little as five minutes of being powered up.



2 Privacy violations will continue to cause economic harm to consumers

Technological advances accelerate price discrimination.

More data means more profiling

The more connected devices consumers use, the more data is collected and added to their profile. Thus, an insurance company might gather information from your usage of a connected car or a fitness tracker when calculating your insurance rate. This scenario is already a reality. For example, John Hancock—one of the largest life insurance companies in the United States — added fitness tracking with wearable devices to all of its policies two years ago and announced a collaboration with Amazon Halo service in August 2020.

Predictive analytics is on the rise

The decreasing cost and growing adoption of AI and machine learning allow businesses to use accumulated consumer data to find patterns and make predictions about our behavior. This rising trend helps businesses to market and sell more efficiently. The problem is that AI- and ML-driven conclusions (and following decisions) might be made against a consumer, resulting in automated, data-driven discrimination. For example, someone may be excluded from receiving a prime-rate credit card because of non-traditional analytic predictors, such as a person's zip code, relationship status, or even social media use.

3 Google's content prioritization engine is accelerating exposure of people's private information

Google rewards data brokers, AKA "people-search sites," for fresh new content and, as such, serves as a major accelerator of private information exposure. Here are the hidden mechanics behind this process:

1. People like to look up other people

Google gets hundreds of millions of search requests for people's names (phones, addresses, etc.) each month. This demand drives the multi-billion dollar people-search industry, which depends on free traffic from Google to survive.

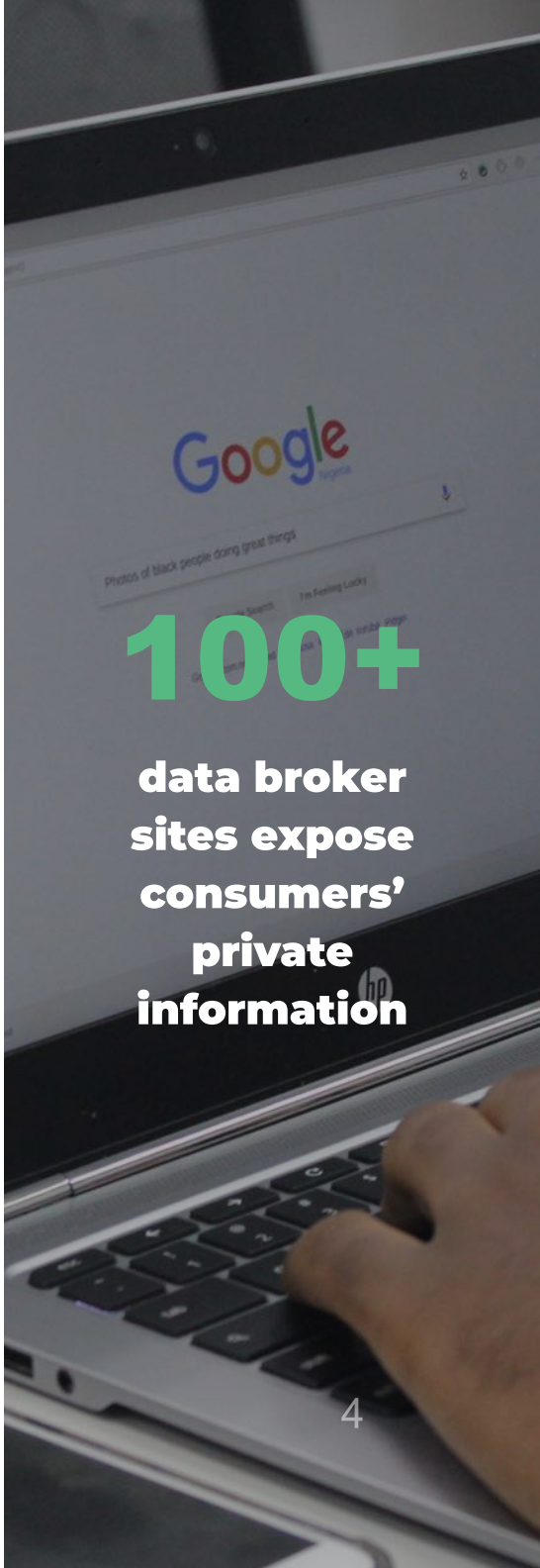
2. The same source of information causes competition

All people-search sites pull personal information from the same source—public records. Google judges the quality of a website's content by how fresh and unique this content is, which poses a major problem for each people-search site.

3. Competition drives exposure

To compete with each other for Google's rankings, people-search sites have to:

- → Release more and more information from public records for free (instead of keeping it behind the paywall).
- → Enrich people's profiles with information from consumer databases (data collected during online browsing and online and offline transactions).

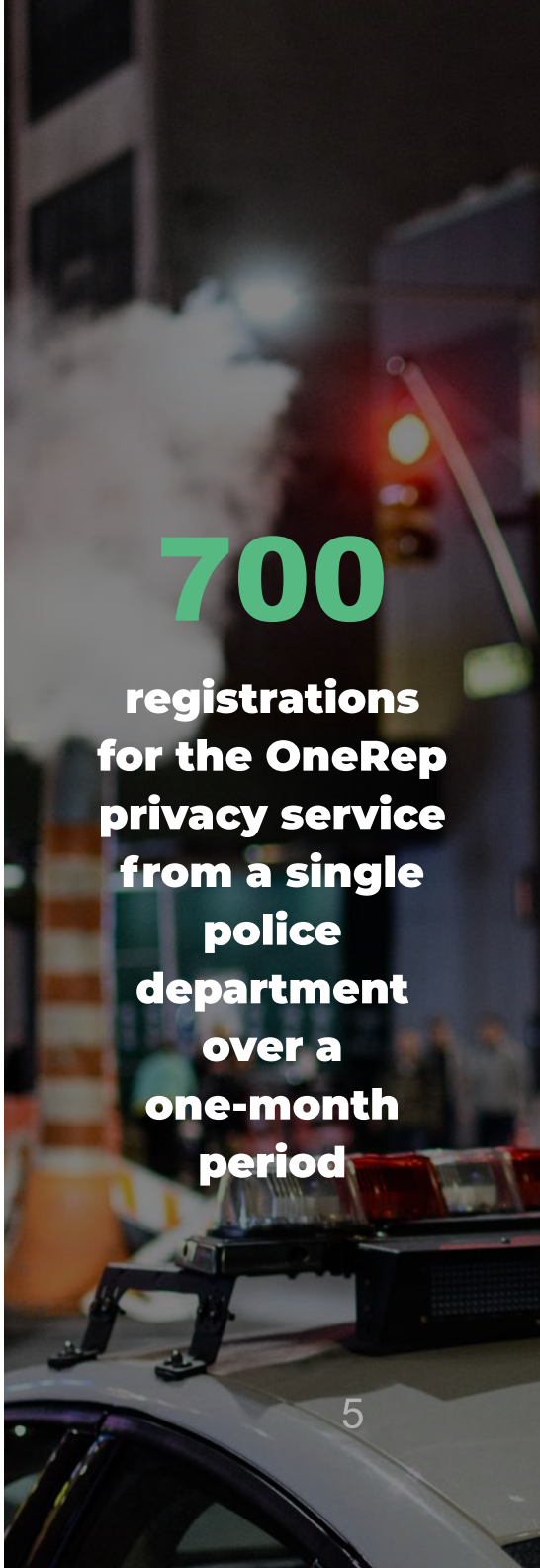


4 Private personal data published online is increasingly being used as a weapon in politicized confrontation

- The horrific assault on Judge Esther Salas's residence over a politically charged issue is unfortunately not an isolated case as the U.S. continues to be politically divided, even post-presidential elections.

- As more personal information is exposed, police, local judges and government officials, as well as private citizens will continue to be increasingly vulnerable. On the OneRep platform, we're seeing a steep increase in registrations from civil workers, reporters, and political activists. For example, in a single month, we saw over 700 registrations for our privacy service from a single police department.

- To put a spotlight on the political affiliation exposure, the people-search site VoterRecords.com has access to 130M voter records; the site gets 4M monthly visitors and is growing. Unfortunately, any people-search site can, and increasingly does, add voter information to people's personal profiles that appear on Google.



5 Online privacy worries keep growing and more people will take action

On the heels of continued scrutiny around social media, people are concerned personal information exposure will cause them harm.

People fear work discrimination

A survey run on the OneRep.com site with over 18,000 respondents revealed that people considered age to be a factor in decreasing their chances of getting hired and increasing their chances of being laid off. In 2018, 15% of respondents selected “colleagues and employers” as the least desired group to see their private information; that number grew to 18% in 2020.

People feel uncomfortable with Google sharing their data

The same survey revealed that in 2018, 7.5% of people felt comfortable with the amount of information Google reveals about them, vs. 6.4% in 2019 and only 4.5% in 2020.

People are increasingly taking a proactive approach to privacy

90% of site visitor responders say they are looking for ways to remove their private information from the internet before the exposure causes them any serious harm, such as identity theft or stalking.

6 The gap between the US legislature and consumer data aggregation is growing

Progress has been made in furthering consumer privacy laws, but we are far from greatness.

Legislation fails to keep pace with technology

Legislators and regulators are unable to keep up with the pace of information collection, growth, and usage. At best, privacy legislation covers a small portion of the issues related to this growth. At worst, they approve and cement a pay-for-privacy approach, such as the recently passed Prop 24 in California.

No federal regulation

The advancement of privacy legislation in the United States is additionally complicated by the historical resistance to implementing a federal law for data privacy. Each state has its own approach to privacy regulation and a nationwide data protection regime is unlikely to happen soon.

47

states have no consumer data privacy laws

No federal-level privacy regulation in the U.S.

7 Privacy as a service is on a growth trajectory

The emergence and success of new startups in the privacy field, such as Mine and Spartacus, is a sign that people are becoming more aware and investors are starting to recognize this growing consumer demand. Some notable recent milestones include:

- Israel-based Mine, a company enabling consumers to reclaim their personal data and reduce personal data privacy risks, launched in the U.S. and raised a $9.5M Series A round of investment.
- MeWe, the California-based privacy-first alternative to Facebook, surged to 9M users. The social network has a Privacy Bill of Rights giving its users total control of their data and privacy.
- The privacy-focused Brave browser grew over 130% in the past year.

The investments and innovation in the consumer privacy space should give us a glimmer of hope towards a safer, better world on- and offline.

Integrate the OneRep privacy protection into your solution

OneRep is a fully automated platform that removes consumers' private records ***from Google and more than 100 people-search sites.***

Why partner

Add value
Bring your customers, partners and employees peace of mind by removing their sensitive information from 100+ sites and Google.

Foster loyalty
80% of OneRep customers stay for over a year.

Integrate easily
Ramp up quickly with well-documented API and dedicated technical support

Who can partner

- Identity Theft Protection companies
- Affinity solutions
- Benefits providers
- Privacy & security consultants

GET IN TOUCH