July 2025

Leiden Model United Nations 2025

The right of individuals to monitor and influence their search algorithms

Special Conference on Freedom of Speech

Table of Contents

Table of Contents **1**
Introduction **2**
Definition of key terms **3**
General Overview **5**
Privacy concerns 6
Misinformation 7
Affecting freedom of speech 7
The right to know 7
Major parties involved **9**
Brazil 9
ChatGPT 9
EU 9
Google Search 10
Other Chromium based or privacy oriented browsers 10
US 11
Timeline of events **12**
Possible solutions **13**
Bibliography **14**

Introduction

Search algorithms are essentially information filtering systems on browser platforms that enable us to navigate the internet. They are tools designed to aid human decision-making in the era of access to vast amounts of information; they predict, filter, and then respond to the searched keyword by presenting users with relevant facts. However, its convenience often leads to blurred boundaries between human and automated decision-making, and more often than not, the exact intricate workings of the search algorithm are kept unknown from the public as trade secrets. The existence of these black-box algorithms largely contributes to the perception that human beings feel that they have no control over, nor do they understand the systems that facilitate their daily digital experience. Indeed, rapid advances in technology raise more questions than solutions regarding policymaking, the privacy and human rights of users, and further concerns regarding data quality, privacy, or potential biases in the workings of algorithms.

As of 2025, there are no global norms in terms of legislation that protects users' right to understand, review and control how search engines and recommendation systems customize results or track user behaviour. Notable regional legislation exists, for instance, the European Union's General Data Protection Regulation (GDPR), which is deemed as an important extension of EU regulation on information privacy and human rights. It aims to enhance users' control and rights over how their personal information is used on online platforms and to simplify the regulations of international businesses. As for the United States, while there is no federal legislation that explicitly addresses the issue of protecting users' rights in search personalization, notable state-level laws, such as the California Consumer Privacy Act, are in power to demand companies accommodate the rights of individuals.

Definition of key terms

Algorithmic secrecy

The deliberate gatekeeping of information about an algorithm's inner workings – its logic, training data, or decision-making criteria – often to protect the private interest of an enterprise.

Algorithmic transparency

The principle that algorithms—especially those affecting individuals—should be open in purpose, structure, and decision-making criteria for users, regulators

Black box algorithms

Algorithmic systems that take inputs and produce outputs without revealing information about how its automated decision-making works.

Browser cookies

Small pieces of data planted on a user's device by the website to record information such as login status or browsing history. Depending on their purpose and scope (first- vs third-party), they often require explicit user consent.

End-to-end encryption (E2EE):

A method to encrypt information at the sending device and only decrypt at the intended recipient device. The message cant be intercepted even if it were received by a third party, including telecommunication service providers.

Intellectual property protection (IP)

Creations of the mind such as inventions, literary or artistic works, designs, that are protected by law from being misused.

Search query

the specific text users enter into search engines to initiate searching.

SEO (search engine optimization)

The practice of improving a website's visibility in organic (unpaid) search results by optimizing content and site structure, based on predictions on how search algorithms rank relevance according to search queries and keywords.

Targeted advertising

Digital marketing strategies that involve delivering advertisements to specific individuals or groups based on their demographics, interests, and online behaviour.

Trade secret

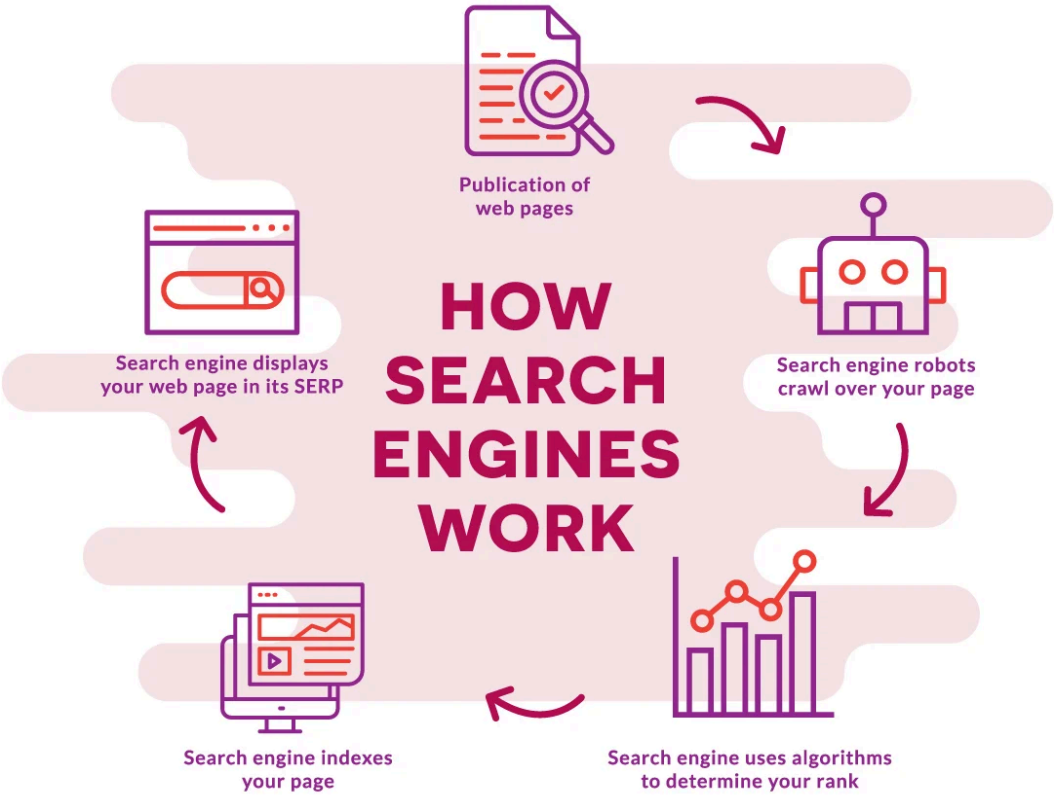
Confidential business information protected by trade law. It usually grants its holder a competitive advantage in the market.

Web analytics

The practice of collecting, measuring, analyzing, and reporting data about website visitor behavior—such as page views, traffic sources, session duration, and conversion metrics—to optimize user experience and marketing effectiveness.

General Overview

The existence of search engines allow users to access a great expanse of information, facilitating research, purchase or daily browsing activities. The user enters a query in a browser, and the browser yields the search engine results page, a list of hyperlinks ranked according to their relevance to the keyword. The engine's rapid response to a query is the result of a complex process of indexing: collecting, analyzing and storing the data on web servers. The database of collected data is regularly updated by automated software systems known as web crawlers, which explores the web and adds new and updated URLs to the index. Vast amounts of webpages exist, and the crawler functions by following hyperlinks on webpages that are already crawled, so some pages may never be discovered. When the content of a webpage is determined as satisfactory to the quality threshold of indexing, the page will be stored and indexed, thus determining the reach and visibility of the page. For digital marketing, it is essential to understand the mechanics behind search engines, since websites can be promoted by adjusting their contents according to the algorithms, thus improving their presence in search.



Ranking algorithms consider several factors attributing the relevance of a search result, with the content type and quality being the most prominent ones, but it also tracks user information such as IP addresses, browsing history (search query histories, click-through history, online fingerprints) and cookies. Based on these recorded data of individuals' browsing pattern, the users can be profiled according to their demographic and their online habits, thus providing means for targeted digital marketing. In more recent trends this process also involves using machine learning to refine the profiling models, using popular techniques such as A/B testing on users. However, the data contained in personal profiles are prone to be abused in ways that threaten or compromise the privacy of users. Personal information may be mined through the use of algorithms, creating a risk of large-scale surveillance ("dataveillance") by private entities or governments alike (Rubinstein, Lee, and Schwartz 2008). Furthermore, when personal profile data is used in ways that differ from its original context, for instance, by creating a personal profile for a specific individual, search engines make it easier to identify information about this user, thus losing the practical obscurity of anonymous data. Another

concern related to the use of algorithms for automated data processing is focused on cloud data storage; in servers where data are not stored on local storage but remotely on the internet, it is difficult for users to ascertain whether their data is under protection using technologies such as strong end-to-end encryption, and whether these data protection methods are altered. In today's regulatory scope, businesses selling consumer data to third parties without the consent of individuals is the aspect most restriction measures focus on.

Since search engine algorithms are tools for humans to gather information, advances in algorithm technology will evidently shift humans' behavioural trends towards their information environment. By collecting personal information for commercial and sometimes political means, users are shown information not actively selected by themselves, but according to the calculations of the algorithms. Besides, with the help of user profiling, an individual will be seen as a cybernetic assemblage consisting of their realistic needs and emotional attitudes in different online scenarios. As Ellen Balka coined the expression "shadow bodies" produced by information systems, the same phenomenon is present in the case of the wide-spread use of search algorithms; some aspects of the user are emphasized while others are overlooked, and the digital profiling will only partially represent the users' preferences. Hence, the slippage between the anticipated user and the user themself will be able to further manipulate the digital habits of users and prove to be politically problematic, or even productive.

Privacy concerns

Organizations like telecommunication companies, e-commerce and social media platforms too frequently utilize the lucrative practice of selling consumer data to third parties. The data collected range from sensitive information, such as healthcare data, to browsing habits, purchase patterns and personal preferences of a user, and can be utilized to create detailed consumer profiles for targeted digital advertising. Fortunately, public awareness about protection of browsing data has increased in the past decade, especially after large-scare criticism online platforms have faced because of their roles in politically motivated acts of selling consumer data to third parties without explicit consent.

For instance, in 2019 Facebook faced public scrutiny for its role in the Facebook-Cambridge Analytica Scandal. In the 2010s, data of Facebook users were collected by the British consulting firm Cambridge Analytica for more precise opportunities for political advertising. The firm was accused of interfering with the Brexit referendum in 2016, as well as advertising in favor of presidential campaigns of the Republican Party. Other uses include targeted advertising on online retail platforms, telecommunication companies sharing location data to third parties.

Since most online platforms serve a global audience, businesses must make sure their data management policies align with stricter data privacy regulations such as GDPR and CCPA. Thus, it is beneficial for both businesses and consumers to apply data and privacy protecting measures. One of the most important tools for this aim is the Consent Management Platform (CMPs), the pop-up page on websites that offers users an opportunity to be informed about what data is being processed, usually classified types of cookies, whether it is targeting, analytical, or strictly needed. Consumers can choose to opt-out, or monitor how they wish to consent to data sharing. With data minimalization, the platforms will only collect the necessary data, thus minimalizing the potential risk if data is misused or hijacked. Another frequent practice is data encryption; data is converted into code to prevent unauthorized access. Most web browsers also provide users with the option to revoke their consent for browsing data to be tracked, and promises that with consent being denied, their analytics algorithms such as meta tags and cookies will be denied.

Misinformation

After the 2016 elections in the USA, public concern has grown to the creation and dissemination of fake news through recommendation algorithms on social media. These platforms and their personalized recommendation algorithms have significant influence on civil decision making processes. And due to increasing public and media awareness, platforms like YouTube have been frequently accused by factchecking groups of failing to combat harmful content that means to spread false information. Its algorithms are prone to amplify negativity and stereotypes, while giving little control for users on what they want to see on their feed, as 70% of videos watched on YouTube originate from recommendations. To tackle issues like this, research suggests balancing personalization with content diversity and user agency, as well as implementing editorial responsibility onto social media platforms.

Affecting freedom of speech

Although the positive impact of search algorithms on freedom of speech is evident and has been repeatedly discussed ever since the emergence of this technology, it is unavoidable that algorithms can potentially harm the freedom of information, the freedom of expression of individuals or minority groups. By nature, search engines will favor content that is deemed more relevant and of higher importance, consequently granting them a broader audience. Content that is not indexed or not ranked highly by the search engine will face drawbacks when trying to reach a large audience. Furthermore, a search algorithm might also be biased towards certain types of content or content creators, thereby risking values such as media pluralism and diversity.

Most social media platforms also deploy algorithmic predictions of user preferences and actively impact the feeds of users and the order in which search results appear. As an example, since YouTube's algorithm is designed to maximize user engagement, watch time and engagement behavior is tracked, thus revealing the immediate satisfaction or intensive emotional reaction. However, researchers argue that optimizing for watch time and similar engagement metrics—which reflect users' immediate satisfaction—may not necessarily correlate with long-term satisfaction or the consumption of high-quality content, thus the algorithm's content suggestions only reflect the impulsive preferences, which may not align with user's long term well-being. Given the size of platforms such as Google or TikTok, their ample capacity to amplify certain voices makes this matter on no account trivial.

The right to know

The expression "right to know" was coined by Associated Press journalist Kent Cooper. In a democratic society, political freedom for all should be facilitated by sufficient information about decisions that affect the people. Generally speaking, the right to know proves to be a legal right protecting public interests concerned with democratic governance, public safety, and social equality. Hence, this right empowers citizens to have knowledge about their major source of information - recommendation algorithms and search engine algorithms. Organizations and journalists have called for algorithmic transparency to be adapted, claiming the societal benefits that can be achieved by users knowing the inputs to the algorithm. Another frequently used term is academic accountability, which implies that organizations that use algorithms must be accountable for the decisions made by those algorithms.

In the case of digital governing, it seems appealingly straightforward to obtain access to the instruments of algorithmic governance; access to source code is necessary to understand how an algorithm works, and public interest serves as perfect justification for disclosure. However, regarding

private enterprises, algorithms are often protected as trade secrets; this is possible because there is proof that real revenue is generated from the use of these algorithms, since recommendation algorithms generate 70% of YouTube's views, and the percentage for TikTok is similarly high. Because of this, private sector vendors succeed in shielding the workings of algorithms from public disclosure, and currently the breadth of any legislation lacks measures to tackle algorithmic secrecy. It is hereby recognised that an inherent tension exists wherein private interests clash with the public interest; consequently, the matter is formally placed under policy review and mandated for consideration by policymakers.

Major parties involved

Brazil

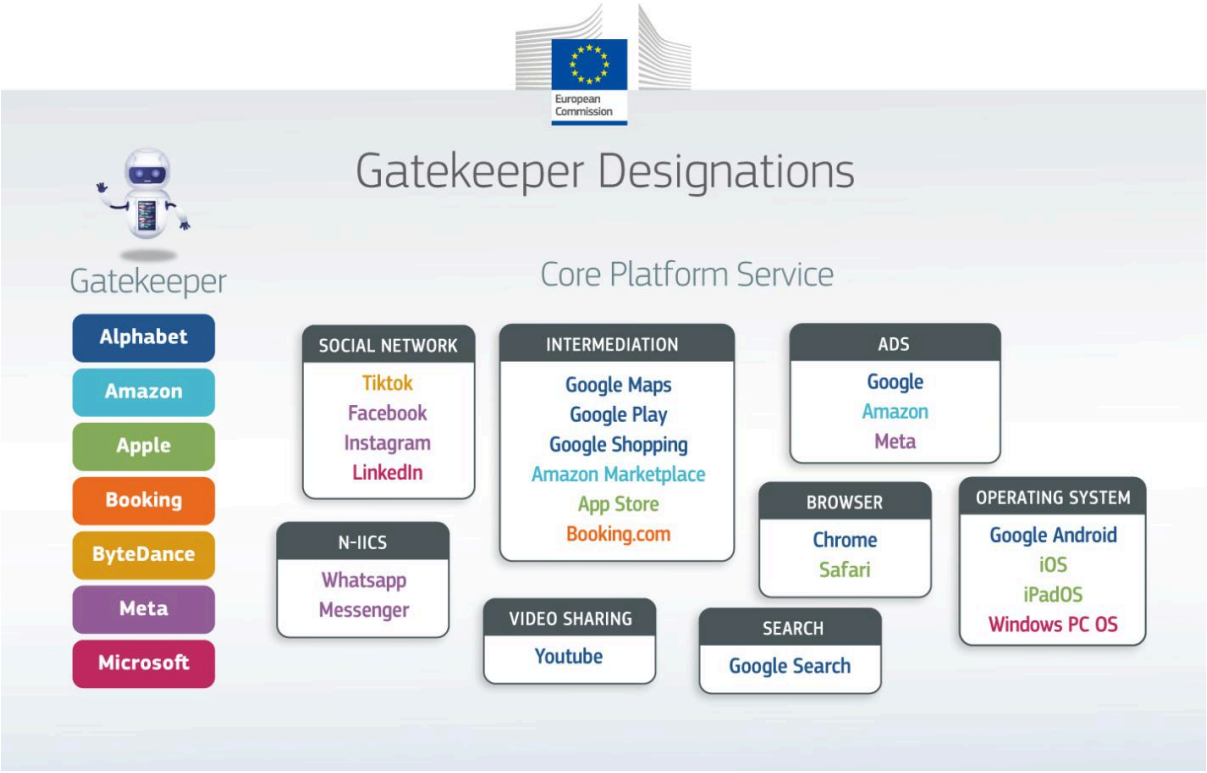
The federal resolution Lei Geral de Proteção de Dados (LGPD, Law 13.709/2018, effective 2020) ensures basic privacy rights for users, including but not limited to regulations on how personal data is processed, how users are granted right to have access and request to delete their data from the database. The newly passed AI bill introduces new rights for individuals when interacting with high-risk AI systems, as well as highlighting the importance of algorithms literacy.

ChatGPT

Released by OpenAI in November 2022, ChatGPT's website is now among the 5 most-visited websites globally by 2025. The chatbot is recognized for its articulate natural language responses and its versatility to answer the needs of the user, its capabilities including answering follow-up questions, debug computer code, analyze or translate text, and summarizing documents. The question-answering ability of ChatGPT posed a threat to traditional search engines, catalyzing a widespread interest in developing generative AI. The chatbot has been criticized for its limitations and potential for unethical use; its algorithmic secrecy, its potential to generate appropriate sounding but actually false information, possible algorithmic bias behind its training data all raised public concern, eventually prompting calls for further regulation of artificial intelligence and algorithmic secrecy.

EU

Among key policies in force of 2025, the European Union provides the strongest protection with the help of a coordinated set of laws: the GDPR serves as a foundation that lays off human rights principles that should be considered when personally identifiable is processed in any way, its charters highlighting the right to privacy (Article 8), the right to reject an inhibited free flow of true information, freedom of expression and assembly and association (Article 10, 11). Furthermore, a milestone in algorithm related policymaking: the right to opt out of data processing (Article 21). Further legislation reinforcements, such as the Digital Services Act (Regulation EU 2022/2065, effective 2024) and Digital Markets Act (Regulation EU 2022/1925, effective 2024) aims to target major digital platform services such as the Google Search and Amazon Marketplace, further protecting user's active right to choose their default search engine and urging firms to publish clear information on how their personalization or recommendation algorithms work.



Google Search

A search engine operated by Google. It is the most popular search engine worldwide, it has a 90% share of the global search engine market, thus holding a de facto monopoly over internet search and search advertising. Google Search operates algorithms to analyze and rank websites based on their relevance to their search query, it is known for its immense index that offers regularly updated information. Ever since Google established its place as an industry giant, Google has been continuously facing criticism and allegations regarding violating antitrust regulations and defying users' privacy principles. For instance, Google Search places long-term cookies on users' machines to store preferences, a mechanism which enables them to store the data for more than a year. Recently, the feature of generating AI summaries in response to search queries was introduced, as a part of Google's efforts to counter the unprecedented threat generative AI technology such as OpenAI's ChatGPT pose. It has been criticized for condensing information from various sources, making it less likely for people to review original articles and websites, further inhibiting content creators to monetize their content. Scientific American has pointed out negative environmental consequences of this new feature, as such a search uses 30 times more energy than a conventional one.

Other Chromium based or privacy oriented browsers

Chromium is a free and open-source web browser project launched alongside the debut of Google Chrome in 2008. The source code for Chromium is freely accessible, it also provides the vast majority of Google Chrome, but Chromium lacks a few key features of Google Chrome. It is a widely used codebase for many browsers including Microsoft Edge, Samsung Internet, Opera, DuckDuckGo and Brave. Some of these browsers advocate for a privacy oriented consumer experience, with features such as automatic web tracker blocking, targeted advertisement blocking, and automatic cookie consent tools (DuckDuckGo). Some of these browsers have remained free and open-source, providing users with a wider choice of alternative browsers than google.

US

Due to a lack of federal law that explicitly addresses search personalization, consumers rights are protected through several state statutes in force. The 2018 California Consumer Privacy Act (CCPA) being the first comprehensive law that protects basic privacy rights of individuals, its example was followed by state-level regulations that mostly came in force during 2023-2024: the California Privacy Rights Act (CPRA, 2023), the Virginia Consumer Data Protection Act (CDPA, 2023), and the Colorado Privacy Act (CPA, 2023). The enlisted state statutes all address the sensitivity of personal information being processed, and also aims to offer users an option to opt out, as well as the right to receive logic explanation behind profiling, although the coverage of these policies vary by location.

Timeline of events

1990 September 10th	The Archie Search Engine is created by Alan Emtage, a computer science student at McGill University in Montreal.
1994 April 20	The WebCrawler, the first search engine that allowed users to search any word in any webpage.
1998	Google officially launches
2000 January 1	Baidu, a Chinese search engine related company is founded.
2009 July 29	Microsoft and Yahoo! announces that Yahoo! Search will be powered by Microsoft Bing
2010	US: Consumer Privacy Bill of Rights is drafted to protect privacy rights with minimal legal force
2013	Google revolutionizes its search algorithm with its Hummingbird update. The algorithm is the first attempt to understand user behaviour.
2016 April	The GDPR is adopted by EU institutions
2018 March	Facebook-Cambridge Analytica data scandal is exposed by media
2018 May 25	The GDPR comes into force
2018	Google launches BERT algorithm: a natural language processing model
2021	Google launches Multitask Unified Model (MUM) that understands and responds to complex search queries
2022	EU adopts DSA, DMA
2022 November 30th	ChatGPT was released, prompting a wave of investment in AI
2023	The CPRA, CDPA and CPA come into force
2025	The EU AI Act comes into force

Possible solutions

A multi-layered governance framework can reconcile the opacity of private platforms with democratic oversight. Explainable AI techniques—including post hoc models like LIME, SHAP, and feature-importance rules—allow users to understand and influence outputs without revealing proprietary code. Algorithmic impact assessments and independent third-party audits, informed by public reporting and institutional controls, create accountability ecosystems beyond internal compliance. At the institutional level, bodies like the European Centre for Algorithmic Transparency (ECAT) enforce mandates under the DSA to assess systemic platform risks, while citizen assemblies, deliberative councils, and participatory platforms—such as Taiwan's vTaiwan, Spain's Decidim, or LiqudFeedback—embed democratic values and public participation in algorithmic governance These processes ensure that policy design and oversight reflect societal concerns, not just corporate interests. In combination, these technical, institutional, and participatory mechanisms equip individuals with real control, oversight, and recourse in the design and deployment of algorithmic systems—while protecting platforms' trade secrets and users' privacy.

Sources

Dwivedi-Yu, J., Wang, Y.-C., Qin, L., Canton-Ferrer, C., & Halevy, A. Y. (2022). Affective signals in a social media recommender system. Proceedings of the 28th ACM SIGKDD Conference on Knowledge Discovery and Data Mining, 2831–2841. https://journals.law.harvard.edu/lpr/wp-content/uploads/sites/89/2024/08/18.1-Right-to-Know-Social-Media-Algorithms.pdf

Rubinstein, I. S. (2008). Data mining and internet profiling: Emerging regulatory and technological approaches. Chicago Unbound. https://chicagounbound.uchicago.edu/uclrev/vol75/iss1/12/

Rodriguez, A., & Rodriguez, A. (2018, January 13). YouTube's recommendations drive 70% of what we watch. Quartz. https://qz.com/1178125/youtubes-recommendations-drive-70-of-what-we-watch

Gilbert, B. (2021, July 7). YouTube's secret algorithm continues to push misinformation on users, from false election fraud claims to conspiracy theories, according to a new study. Business Insider. https://www.businessinsider.com/youtube-algorithm-continues-to-push-misinformation-study-finds-2021-7

Wagner, B. (2017). Study on the human rights dimensions of algorithms. Council of Europe, MSI-NET(2016)06 rev, 3–16.

Habib, H., & Nithyanand, R. (2025). YouTube recommendations reinforce negative emotions.

Data protection laws of the world. (n.d.). DLA Piper. Retrieved August 2, 2025, from https://www.dlapiperdataprotection.com/

Bloch-Wehba, H. (n.d.). Transparency's AI problem. Knight First Amendment Institute. Retrieved August 5, 2025, from https://knightcolumbia.org/content/transparencys-ai-problem

Google Search General. (2024). How search works. YouTube. https://www.youtube.com/playlist?list=PLKoqnv2vTMUN83JWBNM6MoBuBcyqhFNY3

Kobie, N. (2019, October 28). How to delete your Google search history and stop tracking. WIRED. https://www.wired.com/story/how-to-delete-google-search-history-tracking/

Shankland, S. (2020, November 30). Google gets web allies by letting outsiders help build Chrome's foundation. CNET. https://www.cnet.com/tech/mobile/google-gets-web-allies-by-letting-outsiders-help-build-chromes-foundation/