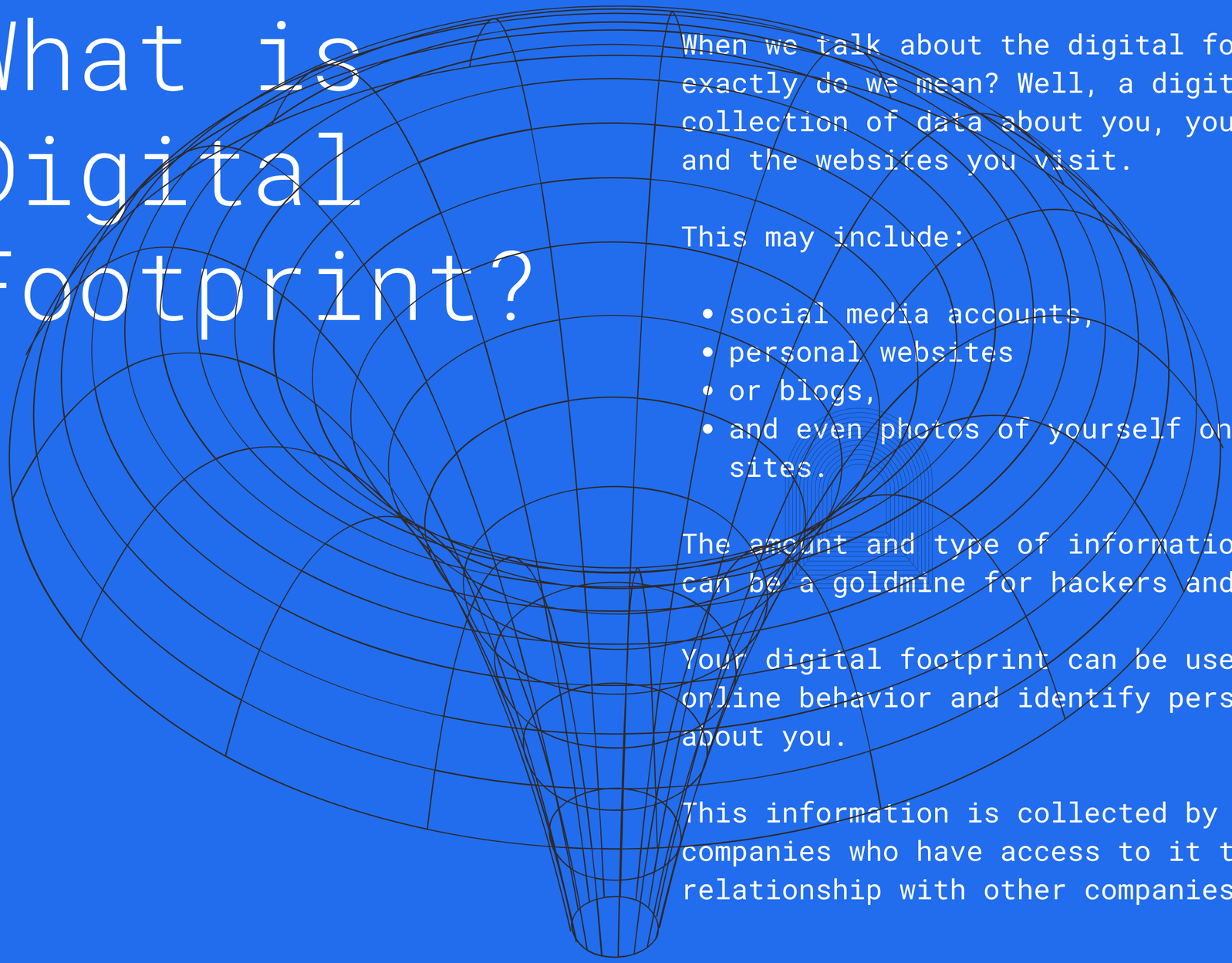
A Guide by
CivFed Legislation Committee

DELETE ME FROM THE INTERNET 101

How to remove your Digital Footprint?

What is Digital Footprint?



When we talk about the digital footprint, what exactly do we mean? Well, a digital footprint is a collection of data about you, your online activity, and the websites you visit.

This may include:

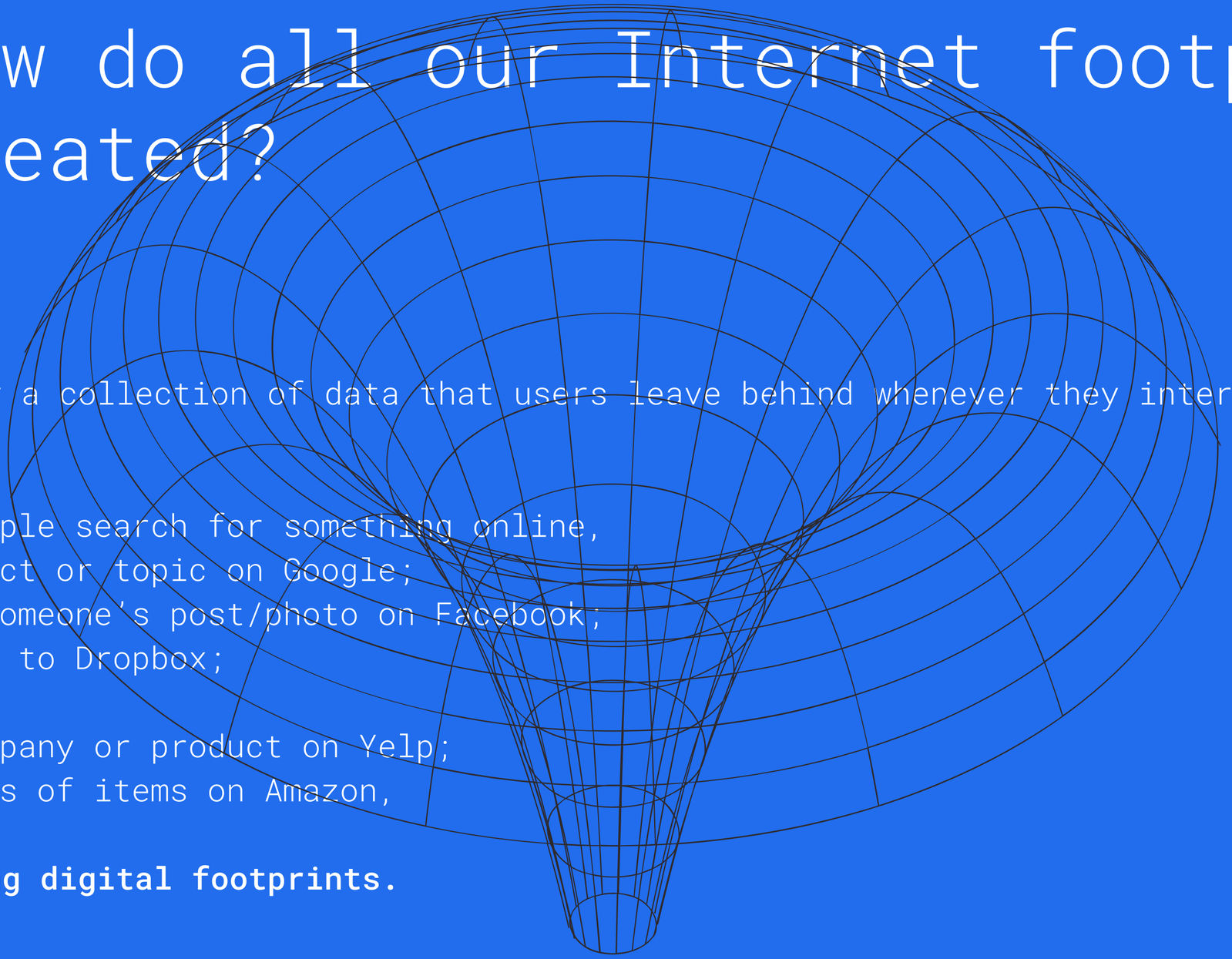
- social media accounts,
- personal websites
- or blogs,
- and even photos of yourself on other people's sites.

The amount and type of information you have online can be a goldmine for hackers and identity thieves.

Your digital footprint can be used to track your online behavior and identify personal information about you.

This information is collected by third-party companies who have access to it through their relationship with other companies.

But how do all our Internet footprints get created?



They are simply a collection of data that users leave behind whenever they interact on the Internet.

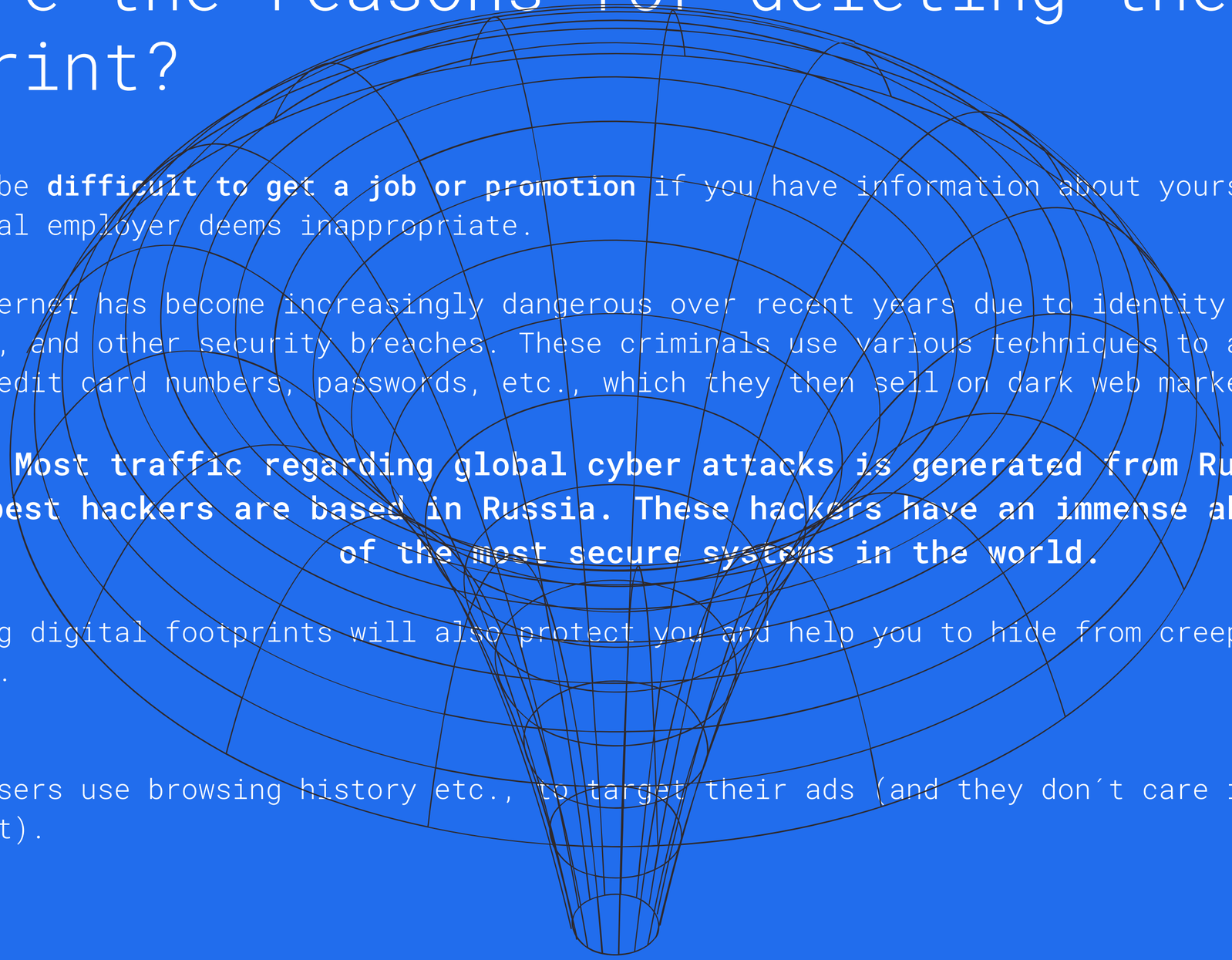
- Whenever people search for something online,
- like a product or topic on Google;
- comment on someone's post/photo on Facebook;
- upload files to Dropbox;
- buy tickets;
- review a company or product on Yelp;
- leave reviews of items on Amazon,

they're creating digital footprints.

So how exactly do these companies collect data about us?

- Companies like Google, Microsoft, etc., send tracking cookies that follow users across different websites and gather information about their interests & preferences.
- They then use this information to provide targeted advertisements that will most likely interest you based on what they know about you from your browsing history or through your online profile details (if connected with a social network).

Why are the reasons for deleting the Digital Footprint?



- It can be **difficult to get a job or promotion** if you have information about yourself online that your potential employer deems inappropriate.

- The internet has become increasingly dangerous over recent years due to identity theft, ransomware attacks, and other security breaches. These criminals use various techniques to access personal data like credit card numbers, passwords, etc., which they then sell on dark web markets for profit.

RUSSIA - Most traffic regarding global cyber attacks is generated from Russia. In fact, some of the best hackers are based in Russia. These hackers have an immense ability to hack some of the most secure systems in the world.

- Deleting digital footprints will also protect you and help you to hide from creepy stalkers or online bullies.

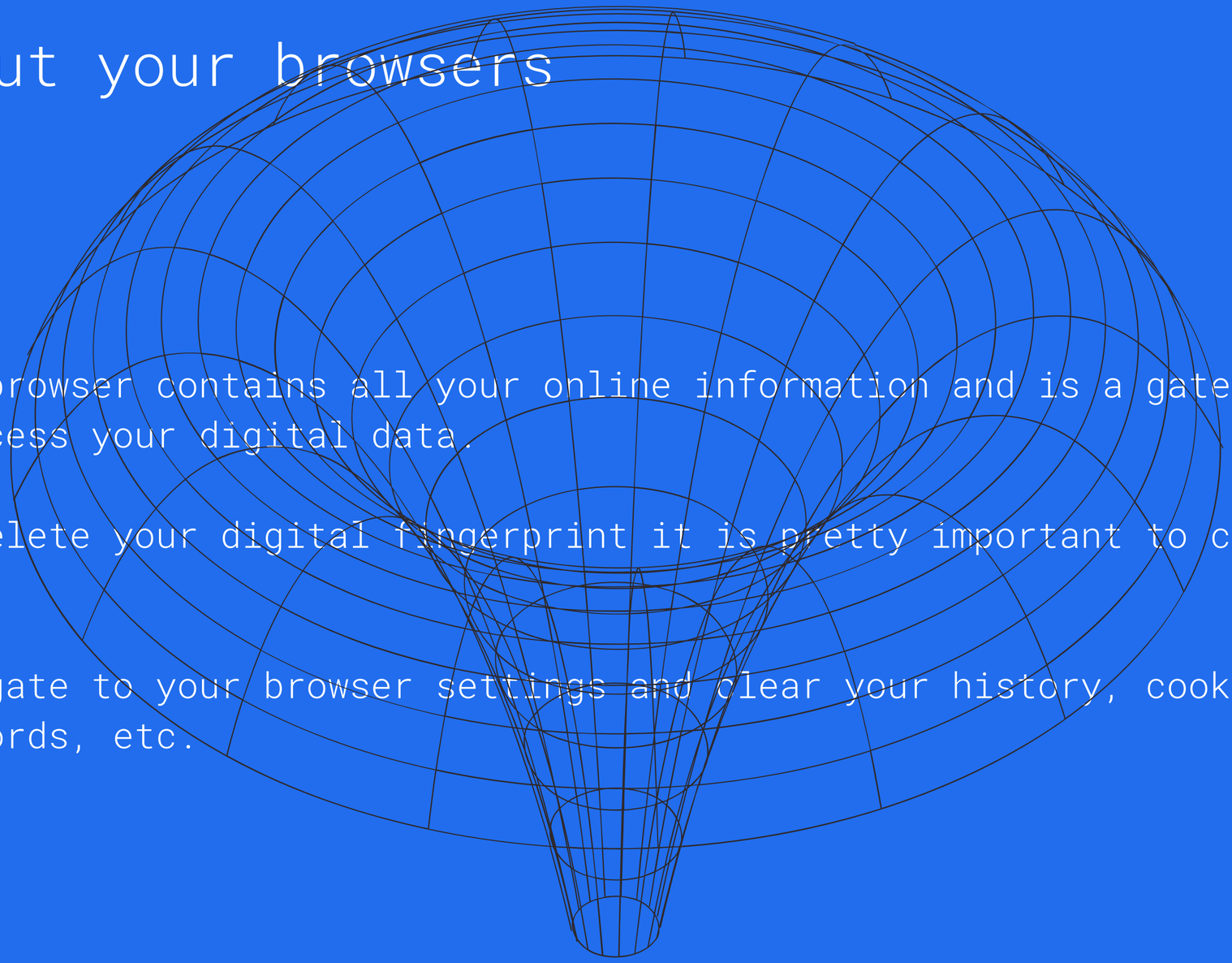
- Advertisers use browsing history etc., to target their ads (and they don´t care if it happens by accident).

How to delete your Digital Footprint completely?

- To remove your digital footprint, you need to first delete all old posts, emails, etc.
- This means that it does take some effort, but the end result is worth it (no one will be able to find any information about you).
- You can use **cleaner programs** too if you're feeling lazy because they do most of the work for you.
- Cleaner Programs: **CCleaner and Total AV**
- **CCleaner Is Disk Cleanup On Steroids**

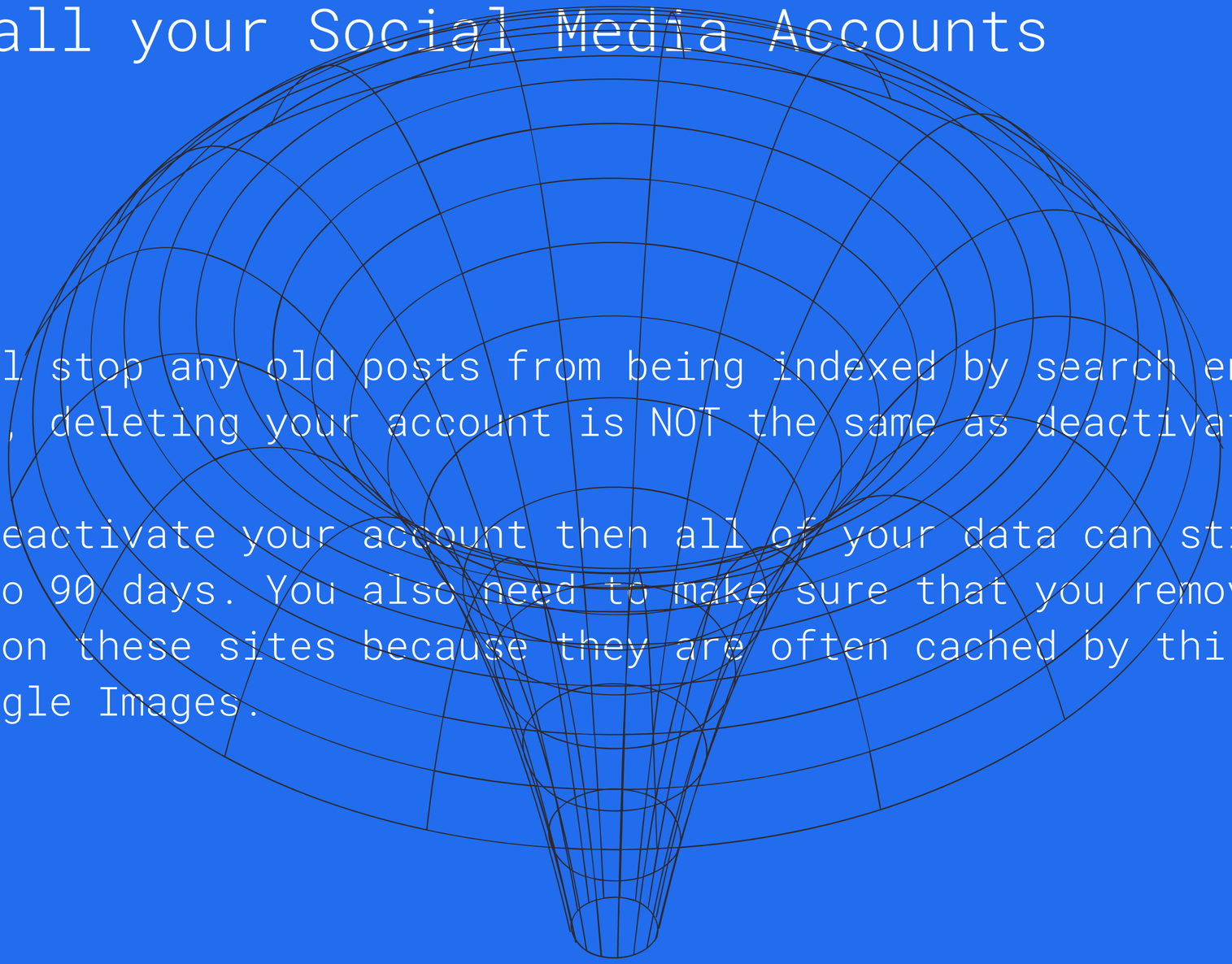
CCleaner has two main uses. One, it scans for and deletes useless files, freeing up space. Two, it erases private data like your browsing history and list of most recently opened files in various programs.

Clear out your browsers



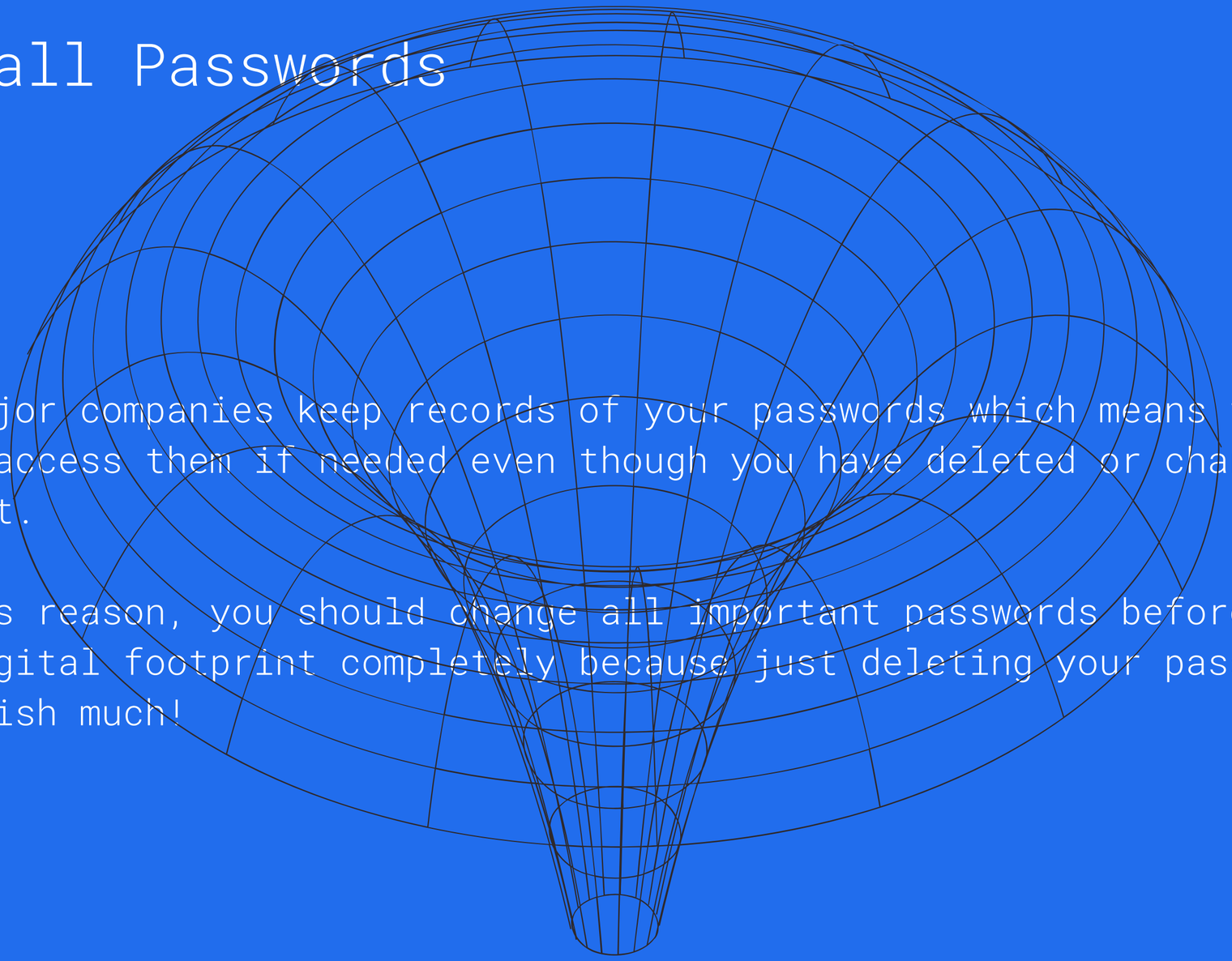
- Your browser contains all your online information and is a gateway for anyone to access your digital data.
- To delete your digital fingerprint it is pretty important to clear browsing data.
- Navigate to your browser settings and clear your history, cookies, saved passwords, etc.

Delete all your Social Media Accounts



- This will stop any old posts from being indexed by search engines. But remember, deleting your account is NOT the same as deactivating it!
- If you deactivate your account then all of your data can still be accessed for up to 90 days. You also need to make sure that you remove every single picture on these sites because they are often cached by third-party websites like Google Images.

Delete all Passwords



- Most major companies keep records of your passwords which means they could easily access them if needed even though you have deleted or changed them in the past.
- For this reason, you should change all important passwords before erasing your digital footprint completely because just deleting your password won’t accomplish much!

Remove personal info from websites

- This is a tricky one that takes time, but if you really want to remove your digital footprint, then it's well worth it.
- The idea is basically to contact any websites where you have shared personal details and ask them to remove this information from their databases.
- This can sometimes involve sending letters in the mail, so make sure you follow up because not all companies will delete your data after just one request.

Note: GPDR would address this!

Unsubscribe yourself from Mailing Listsites

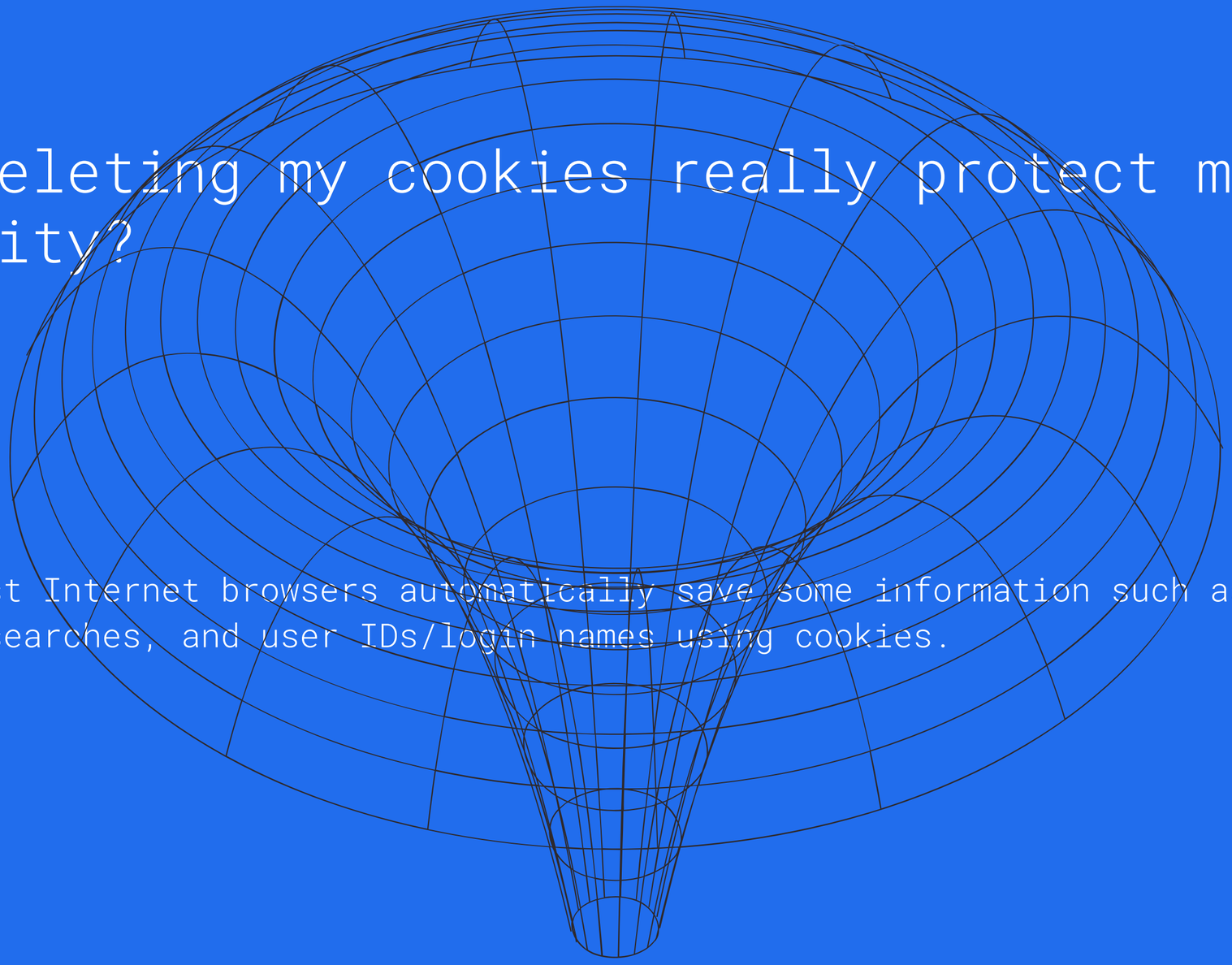
- Most companies use mailing lists to send you advertisements which they compile by pulling your data from multiple places. If you want to remove yourself entirely, this is the important step you need to take.

- However, it can be pretty difficult to unsubscribe yourself from every list manually one by one. So, for that, you can use **Unroll.me**. It would help you to see the list of all your subscription emails and allow you to easily unsubscribe from each service without any hassles.

Delete your Google Activity

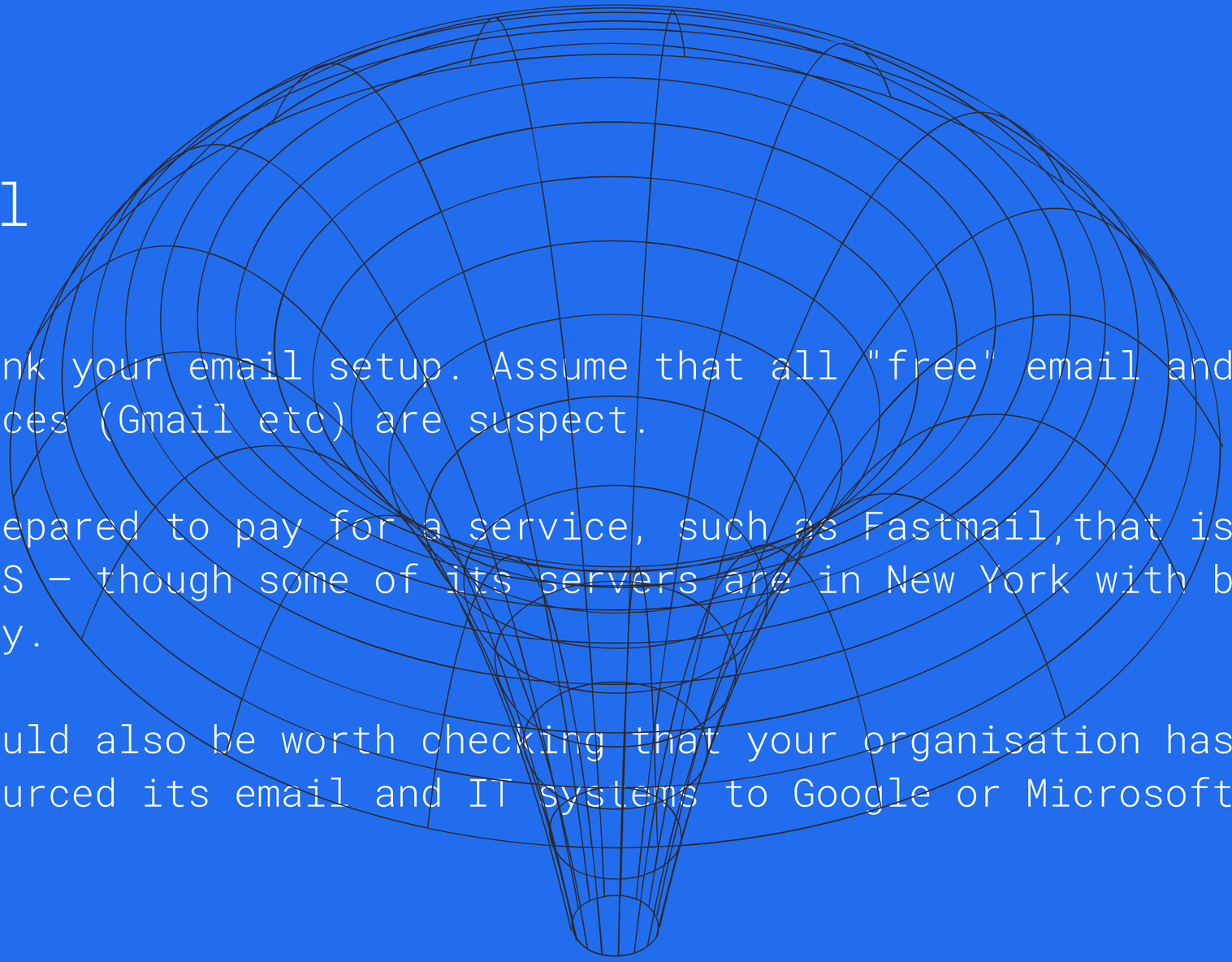
- Right after you create an account on Google, it monitors and records almost everything you do on the web. Just deleting the search history is not enough to remove your digital footprint.
- To completely eradicate it, you need to delete all your Google activities.
- Log into Google and go to “My activity” – https://www.google.com/myactivity – this page shows all the information that Google has logged about your activity online

Can deleting my cookies really protect my identity?



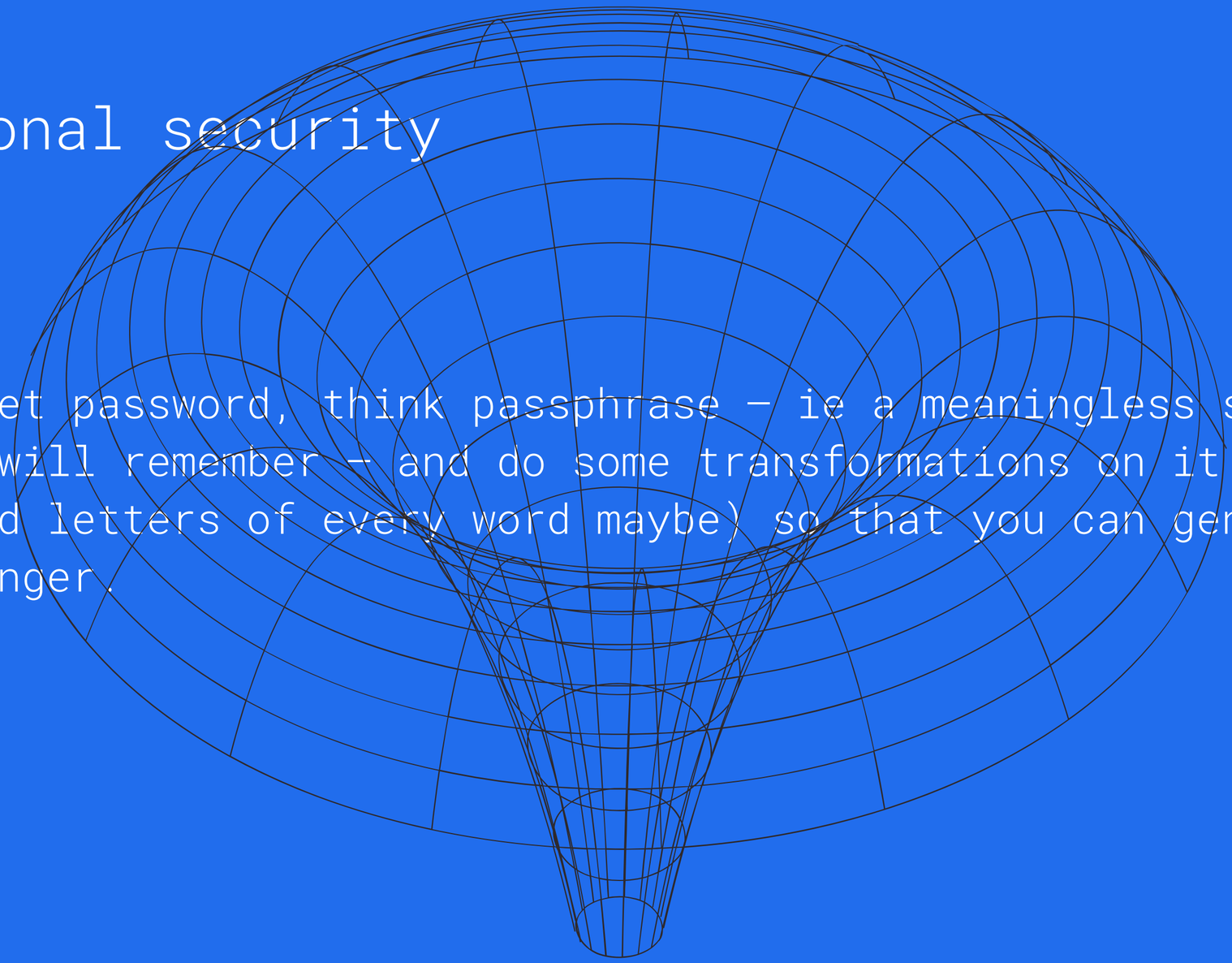
Yes! Most Internet browsers automatically save some information such as bookmarks, recent searches, and user IDs/login names using cookies.

Email



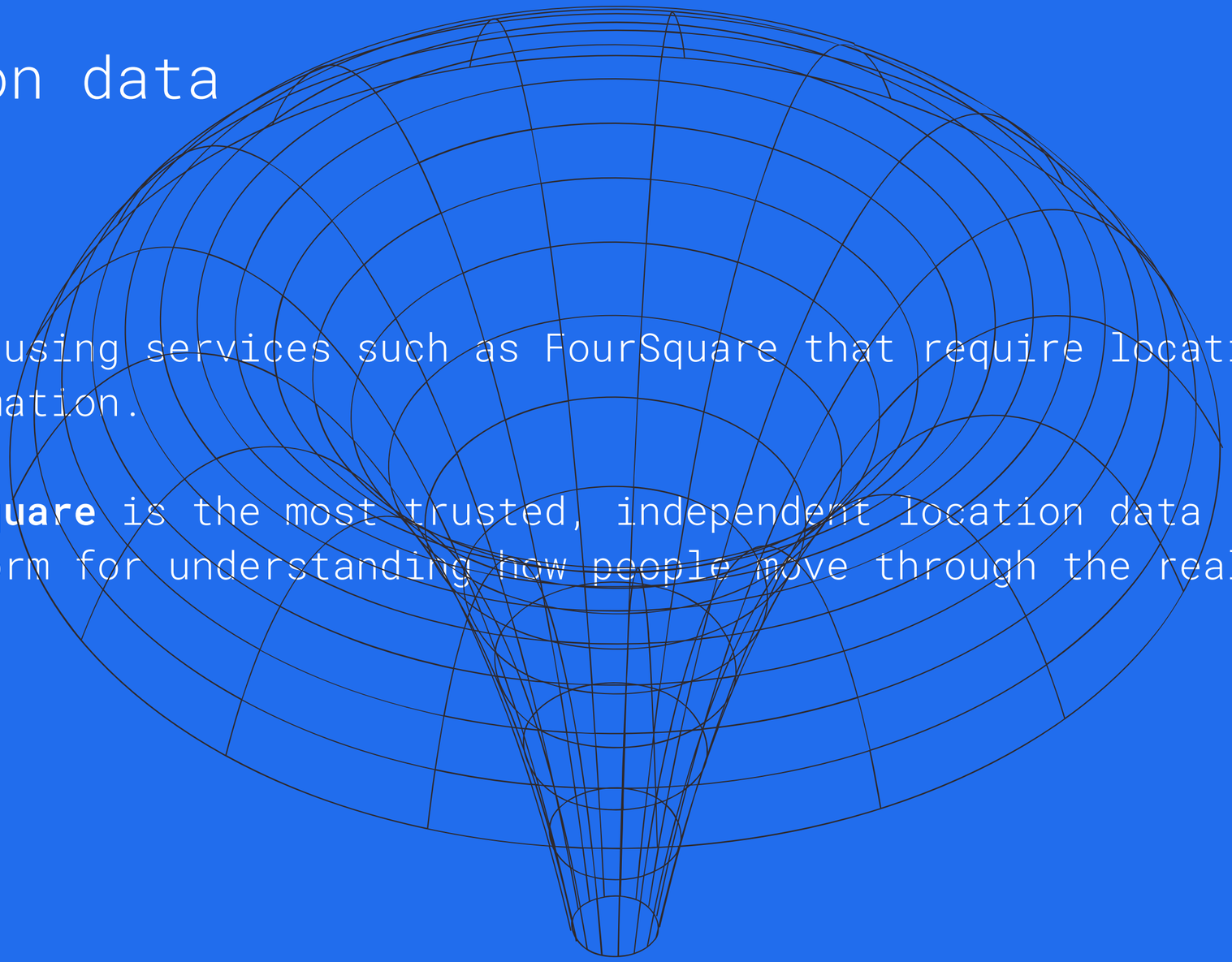
- Rethink your email setup. Assume that all "free" email and webmail services (Gmail etc) are suspect.
- Be prepared to pay for a service, such as Fastmail, that is not based in the US — though some of its servers are in New York with backups in Norway.
- It would also be worth checking that your organisation has not quietly outsourced its email and IT systems to Google or Microsoft.

Personal security



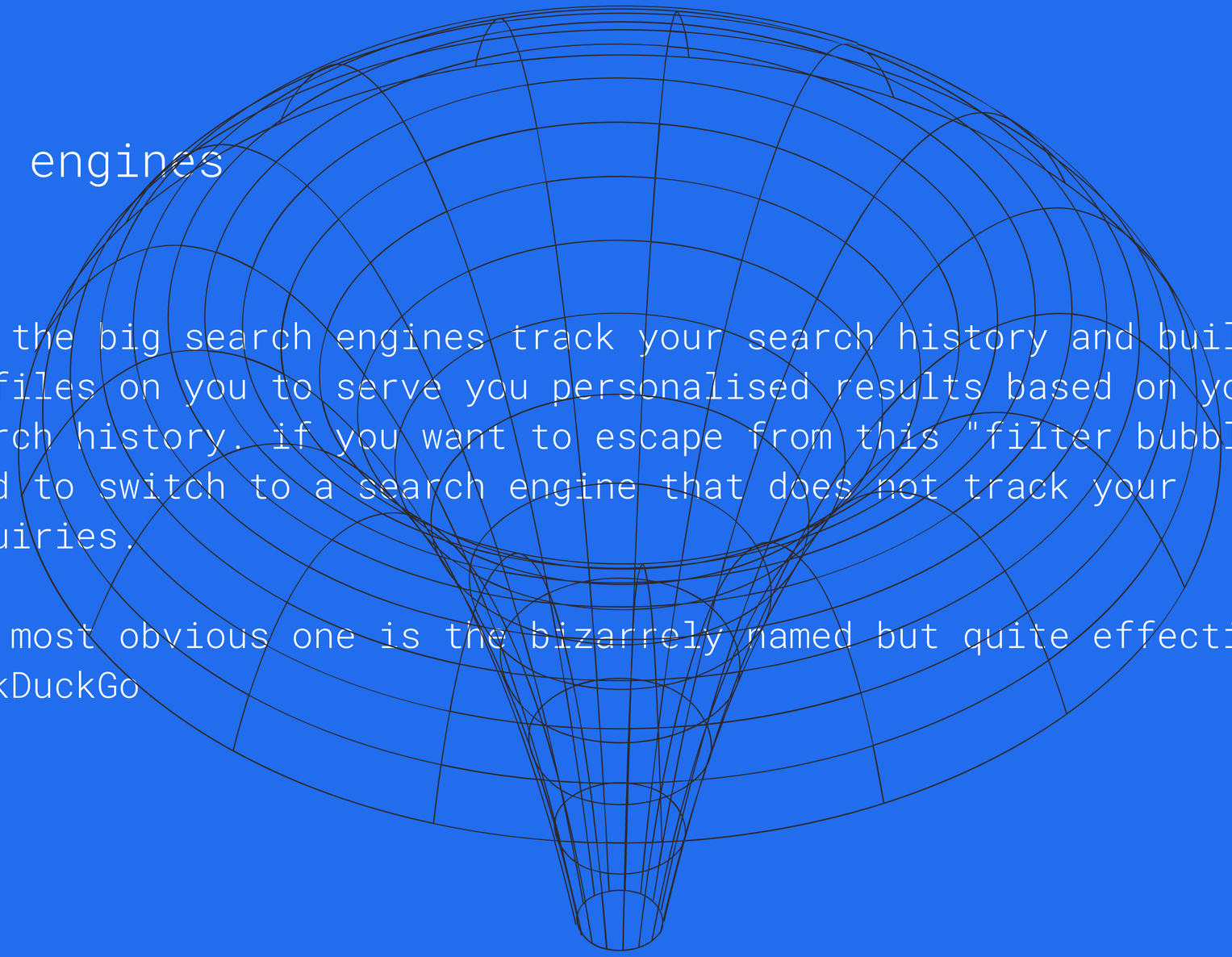
- Forget password, think passphrase – ie a meaningless sentence that you will remember – and do some transformations on it (first and third letters of every word maybe) so that you can generate a stronger.

Location data



- Avoid using services such as FourSquare that require location information.
- **Foursquare** is the most trusted, independent location data platform for understanding how people move through the real world.

Search engines

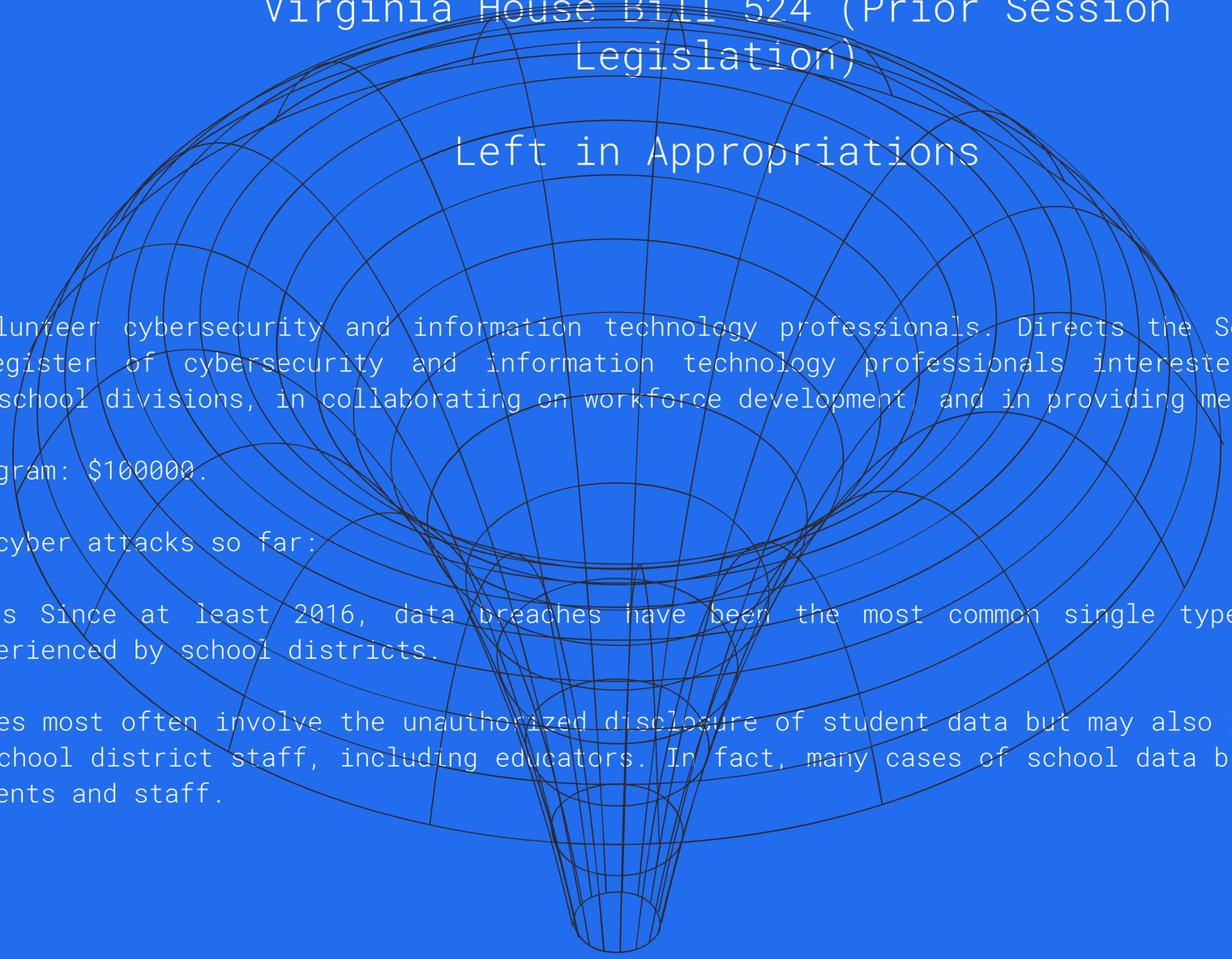


- All the big search engines track your search history and build profiles on you to serve you personalised results based on your search history. if you want to escape from this "filter bubble" you need to switch to a search engine that does not track your inquiries.

- The most obvious one is the bizarrely named but quite effective DuckDuckGo

Virginia House Bill 524 (Prior Session Legislation)

Left in Appropriations

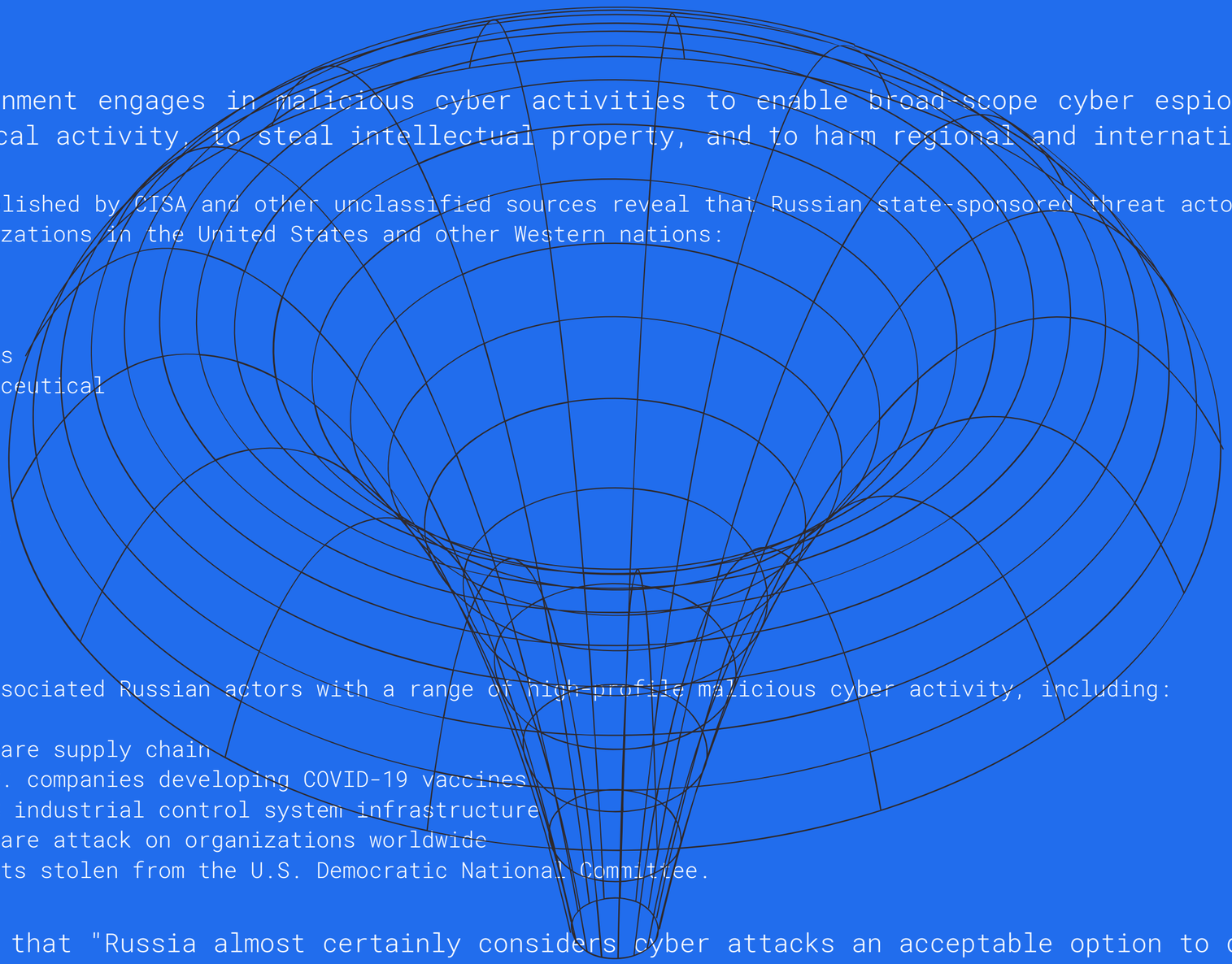


- Summary

Register of volunteer cybersecurity and information technology professionals. Directs the Secretary of Administration to establish a register of cybersecurity and information technology professionals interested in volunteering to assist localities and school divisions, in collaborating on workforce development, and in providing mentorship opportunities.

- Cost for Program: $100000.
- Cost of the cyber attacks so far:
- Data Breaches Since at least 2016, data breaches have been the most common single type of publicly-disclosed cyber incident experienced by school districts.
- These breaches most often involve the unauthorized disclosure of student data but may also include significant amounts of data about school district staff, including educators. In fact, many cases of school data breaches involve sensitive data on both students and staff.

Russia Cyber Threat Overview and Advisories



- The Russian government engages in malicious cyber activities to enable broad-scope cyber espionage, to suppress certain social and political activity, to steal intellectual property, and to harm regional and international adversaries.

- Recent Advisories published by CISA and other unclassified sources reveal that Russian state-sponsored threat actors are targeting the following industries and organizations in the United States and other Western nations:

- COVID-19 research
- governments
- election organizations
- healthcare and pharmaceutical
- defense
- energy
- video gaming
- nuclear
- commercial facilities
- water
- aviation
- manufacturing

- The same reporting associated Russian actors with a range of high-profile malicious cyber activity, including:

- 2020 SolarWinds software supply chain
- 2020 targeting of U.S. companies developing COVID-19 vaccines
- 2018 targeting of U.S industrial control system infrastructure
- 2017 NotPetya ransomware attack on organizations worldwide
- 2016 leaks of documents stolen from the U.S. Democratic National Committee.

- Assessment states that "Russia almost certainly considers cyber attacks an acceptable option to deter adversaries, control escalation, and prosecute conflicts."

- ZHANGJIAKOU, China — Viewers who tuned in to the English-language version of CNN on Chinese television one night shortly after the Olympic Opening Ceremony would have seen Jake Tapper excoriating China for its human rights violations and authoritarian rule.

- When Tapper mentioned Chinese president Xi Jinping, the screen was suddenly replaced with color bars and the message “No Signal Please Stand By.” The signal resumed moments later, as Tapper was wrapping up his remarks.

- Western journalists in China for the Olympic Games are finding it impossible to access services such as Twitter, YouTube, Instagram and Google on local wi-fi networks.

- Even an Olympics-only wifi has restrictions; local search engines do not return results for the Washington Post and the New York Times, for example, and all Yahoo sports and news articles are blocked on every network.

- It’s all part of China’s concerted and thorough effort to block off internet access to certain elements of the outside world, like social media, alternative views and Western philosophies. There’s little recourse for China’s citizens to get to that content, even if they know it exists. VPNs — virtual private networks, designed to get around the so-called “Great Firewall” — are illegal to operate in China.

- So when raised-in-America-but-skiing-for-China gold medalist Eileen Gu blithely advocated for the use of a VPN in an Instagram post, it didn’t go over well with some of her instagram followers or the Chinese government.

- Gu’s Instagram page is a collection of motivational and inspirational slogans, a scrapbook designed to present a specific, curated image of her to the world. One user commented on an otherwise innocuous post:

- “Why can you use Instagram and millions of Chinese people from mainland cannot, why you got such special treatment as a Chinese citizen. That’s not fair, can you speak up for those millions of Chinese who don’t have internet freedom,” user “cilla chan” wrote.

“**Anyone can download a vpn,” Gu replied, “it’s literally free on the App Store”.**

VPN Plus Tor (your next steps)

GDPR

TERRITORIAL SCOPE

EU Establishments

Non-EU Established Organizations
Offer goods or services or engaging in monitoring within the EU.

THE PLAYERS

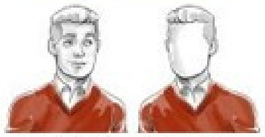
Data Subjects

Data Controllers

Data Processors

Supervisory Authorities

PERSONAL DATA



Identified — Identifiable

SENSITIVE DATA

Racial or Ethnic Origin

Religious or Philosophical Beliefs

Political Opinions

Trade Union Membership

Sex Life

Genetic Data

Biometric Data

Health

RESPONSIBILITIES OF DATA CONTROLLERS AND PROCESSORS

Security

Data Protection Officer (DPO)
Designate DPO if core activity involves regular monitoring or processing large quantities of personal data.

Record of Data Processing Activities
Maintain a documented register of all activities involving processing of EU personal data.

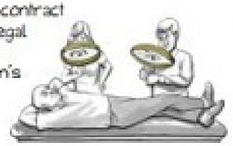
Data Impact Assessment
For high risk situations

Data Protection by Design
built in starting at the beginning of the design process

LAWFUL PROCESSING

Collection and processing of personal data must be for "specified, explicit and legitimate purposes" – with consent of data subject or necessary for

- performance of a contract
- compliance with a legal obligation
- to protect a person's vital interests
- task in the public interest
- legitimate interests



CONSENT

Consent must be freely given, specific, informed, and unambiguous.

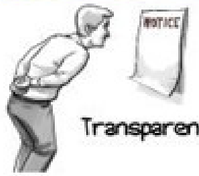
DATA BREACH NOTIFICATION

A *personal data breach* is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."

If likely to result in a high privacy risk → notify data subjects

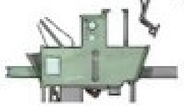
Notify supervisory authorities no later than 72 hours after discovery.

RIGHTS OF DATA SUBJECTS



Transparency

Automated Decision Making



"Right not to be subject to a decision based solely on automated processing, including profiling."

Right to Erasure

Access and Rectification

Purpose Specification and Minimization

Right to Data Portability

ENFORCEMENT

Fines

Up to 20 million euros or 4% of total annual worldwide turnover. Less serious violations: Up to 10 million euros or 2% of total annual worldwide turnover.

Effective Judicial Remedies:
compensation for material and non-material harm.

INTERNATIONAL DATA TRANSFER

Adequate Level of Data Protection

Binding Corporate Rules (BCRs)

Privacy Shield

Model Contractual Clauses

TEACHPRIVACY www.teachprivacy.com

Workforce awareness training by Prof. Daniel J. Solove

7 Guiding Principles of GDPR

Data Minimisation

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which those data is processed.

Purpose Limitation

Personal data may only be collected for the specified, explicit and legitimate purposes and must not be further processed in a manner that is incompatible with those purposes.

Lawful, Fair & Transparent

It must be clearly explained to the data subject that data is being captured & what that data is; why that data is being captured, and by whom, and what will happen to that data. It must also be clear what rights the data subject has regarding their own data.

Accuracy

Personal data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

Storage Limitation

Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; it may be stored for longer periods solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

Integrity and Confidentiality

Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measure.

Accountability

The controller shall be responsible for, and be able to demonstrate compliance with, the GDPR principles.

From the Dark Web

What We Found

Activity

Exposure of Your Data

Source

A list on the dark web

Description

info_outline

In February 2021, a password you use (or previously used) was discovered as part of a combo list in the underground marketplace known the dark web. If you don't know where you used this password, consider the accounts you have: such accounts could include your banking app, health insurance site, social media account, online stores, etc. You would have used this password in combination with your username, as below.

For security reasons, we do not display your entire password. Once we verify that the email address listed below belongs to you, your password will be partially unmasked and displayed.

Be safe always!

ronhaddox@hushmail.com
-add subject line: civfed delete me