Negative: XKeyScore

By “Coach Vance” Trefethen

***Resolved: The United States federal government substantially reform the use of Artificial Intelligence technology***

Case Summary: The AFF plan bans the National Security Agency from using XKeyScore. It’s a program that collects lots of data from the internet, aggregates it, and allows analysts to run queries on it to find out information about people. XKeyScore is a lot more than AI, so Affirmatives don’t really have jurisdiction to abolish it. And most of the details are secret, so we really don’t know whether there’s sufficient justification for abolishing it right now. Between 2014 and 2020 there was an oversight committee that investigated XKeyScore. The majority submitted a (secret, classified, unpublished) report to Congress. Nobody knows what it said but we know it didn’t recommend abolishing XKeyScore. How do we know? Because one of the minority dissenters on the committee (Travis LeBlanc) also published an unclassified commentary on the report, in which he said the majority were not critical enough of the program (he couldn’t have said that if the secret report had recommended abolishing XKeyScore). LeBlanc says the majority did a shoddy job of only halfway investigating it, and missed key issues. One of the key things they missed, according to LeBlanc, was investigating XKeyScore’s use of AI. He says we need a lot more study to really figure out what’s going on. This brief offers a Negative counterplan to do just that. Negative philosophy is that AFF is rushing into a policy change without enough information to make the right decision. Study it according to LeBlanc’s recommendations and then in 3 years have Congress do whatever the new study recommends (nothing, or reform, or abolish).

Suggested strategy: Read the first 3 pages of this brief in the 1NC. Then run the Harm and Solvency responses from later in the brief in 2NC and let 1NR respond to 2AC’s answers to the Counterplan.

Negative: XKeyScore Counterplan 3

NEGATIVE PHILOSOPHY 3

EXTRA-TOPICALITY 3

1. XKeyscore is computer hacking 3

2. XKeyscore is collection of communications 3

3. XKeyscore uses simple database queries 3

4. XKeyscore tracks people using “cookies” - which are not AI (they’re a standard part of every web page) 4

5. The Impact: Plan cannot solve the harms while staying within the resolution 4

HARMS / SIGNIFICANCE 4

1. More study needed about the harms 4

Minority Report says “More Study.” Oversight board member says we need more study before deciding a policy 4

The majority report was a 6-year study of KEYSCORE. Its findings are classified, but we know they didn’t recommend abolishing KEYSCORE because Mr. Leblanc says they weren’t critical enough 5

COUNTERPLAN – Conduct more thorough study 5

XKEYSCORE may need reform, but the best qualified source – the Oversight Board – didn’t study it thoroughly enough 5

Counterplan mandates 5

Reasons to prefer the Counterplan 5

2N / Rebuttal backup: XKeyScore 6

INHERENCY 6

Existing safeguards protect privacy 6

NSA uses multiple layers of safeguards to protect privacy and civil liberties 6

HARMS / SIGNIFICANCE 6

No evidence of harm specifically from AI + more study needed 6

The 6-year oversight board study never scrutinized the use of AI on XKEYSCORE 6

Not enough study has been done on XKeyscore AI to know if it violates 4th Amendment privacy for US citizens 6

Reasons to prefer our evidence: Classified access is the best evidence 6

Americans’ privacy not harmed 7

Questionable activities were actually just typos or minor mistakes, not systemic abuses 7

Privacy doesn’t matter anyway 7

Most people don’t care about privacy as much as they claim to 7

What people value is “security,” not privacy. Strong belief in data privacy is dead 7

Naïve to expect privacy any more, and people’s behavior proves they don’t really care 7

COUNTERPLAN BACKUP 8

Sen. Wyden agrees: We need more information, we know far too little about it 8

Funding: $20 billion in extra money in the Title 1 Education budget this year 8

SOLVENCY 8

1. Everyone else is doing it – you won’t get your privacy back 8

Lots of other agencies and governments are doing the same thing XKEYSCORE is doing 8

2. New Zealand 8

Link: New Zealand uses XKEYSCORE too 8

Link: New Zealand shares intel with the U.S. 9

Solvency Fail: The day after the AFF plan takes effect, the US government just asks New Zealand for all the same info 9

3. Other NSA programs 9

NSA “MUSCULAR” program. It isn’t regulated by the AFF plan, so they’ll use that instead 9

4. Privacy is a problem too big to be solved 9

There’s nothing anyone can do about data privacy other than go back to the Stone Age 9

Negative: XKeyScore Counterplan

NEGATIVE PHILOSOPHY

The Negative position is that the harms of XKEYSCORE have not yet been proven and need more study. We also contend that the Affirmative plan won’t solve the harms anyway and exceeds the boundaries of the resolution. We will offer a counterplan that will take a more careful approach to the problem, if the harms exist at all.

EXTRA-TOPICALITY

 “Extra-Topicality” means that while the Affirmative Plan may do some things that are in the resolution, it does other things, extra policies and mandates, that are not in the resolution. Those “extra” things are not supposed to be part of our debate this year and should be thrown out of the round. The Affirmative Plan contains one part that involves AI, and most of the rest of the Plan deals with other things that are not AI. Those other things need to be dropped from the Affirmative’s Plan and their Advantages. They can change AI and only AI. The problem is…

1. XKeyscore is computer hacking

Morgan Marquis-Boire, Glenn Greenwald and Micah Lee 2015 (journalists) 1 July 2015 THE INTERCEPT “XKEYSCORE – NSA’s Google for the World’s Private Communications” <https://theintercept.com/2015/07/01/nsas-google-worlds-private-communications/> (accessed 7 Feb 2022)

XKEYSCORE plays a central role in how the U.S. government and its surveillance allies hack computer networks around the world. One top-secret 2009 NSA document describes how the system is used by the NSA to gather information for the Office of Tailored Access Operations, an NSA division responsible for Computer Network Exploitation (CNE) — i.e., targeted hacking.

2. XKeyscore is collection of communications

Morgan Marquis-Boire, Glenn Greenwald and Micah Lee 2015 (journalists) 1 July 2015 THE INTERCEPT “XKEYSCORE – NSA’s Google for the World’s Private Communications” <https://theintercept.com/2015/07/01/nsas-google-worlds-private-communications/> (accessed 7 Feb 2022)

These newly published documents demonstrate that collected communications not only include emails, chats and web-browsing traffic, but also pictures, documents, voice calls, webcam photos, web searches, advertising analytics traffic, social media traffic, botnet traffic, logged keystrokes, computer network exploitation (CNE) targeting, intercepted username and password pairs, file uploads to online services, Skype sessions and more.

3. XKeyscore uses simple database queries

Morgan Marquis-Boire, Glenn Greenwald and Micah Lee 2015 (journalists) 1 July 2015 THE INTERCEPT “XKEYSCORE – NSA’s Google for the World’s Private Communications” <https://theintercept.com/2015/07/01/nsas-google-worlds-private-communications/> (accessed 7 Feb 2022)

XKEYSCORE allows for incredibly broad surveillance of people based on perceived patterns of suspicious behavior. It is possible, for instance, to query the system to show the activities of people based on their location, nationality and websites visited. For instance, one slide displays the search “germansinpakistn,” showing an analyst querying XKEYSCORE for all [individuals in Pakistan visiting specific German language message boards](https://www.documentcloud.org/documents/2116488-xks-targets-visiting-specific-websites.html#document/p1).

4. XKeyscore tracks people using “cookies” - which are not AI (they’re a standard part of every web page)

Morgan Marquis-Boire, Glenn Greenwald and Micah Lee 2015 (journalists) 1 July 2015 THE INTERCEPT “XKEYSCORE – NSA’s Google for the World’s Private Communications” <https://theintercept.com/2015/07/01/nsas-google-worlds-private-communications/> (accessed 7 Feb 2022)

When intelligence agencies collect massive amounts of Internet traffic all over the world, they face the challenge of making sense of that data. The vast quantities collected make it difficult to connect the stored traffic to specific individuals. Internet companies have also encountered this problem and have solved it by tracking their users with identifiers that are unique to each individual, often in the form of browser cookies. Cookies are small pieces of data that websites store in visitors’ browsers. [**END QUOTE**] They are used for a variety of purposes, including authenticating users (cookies make it possible to log in to websites), storing preferences, and uniquely tracking individuals even if they’re using the same IP address as many other people. Websites also embed code used by third-party services to collect analytics or host ads, which also use cookies to track users. According to [one slide](https://www.documentcloud.org/documents/2115979-advanced-http-activity-analysis.html#document/p52), “Almost all websites have cookies enabled.” The NSA’s ability to piggyback off of private companies’ tracking of their own users is a vital instrument that allows the agency to trace the data it collects to individual users. [**THEY GO ON LATER IN THE SAME CONTEXT QUOTE**:] It makes no difference if visitors switch to public Wi-Fi networks or connect to VPNs to change their IP addresses: the tracking cookie will follow them around as long as they are using the same web browser and fail to clear their cookies.

5. The Impact: Plan cannot solve the harms while staying within the resolution

Even if you believe your privacy is being violated by XKeyscore, you wouldn’t go home tonight sleeping better if you knew your Affirmative ballot allowed the government to continue collecting your communications, tracking your web browser cookies, hacking your computer and querying any information they have about you in their database…. As long as they don’t use AI to analyze any of it. The harms of privacy violation happen before AI gets involved. Stopping AI doesn’t stop the harms, but that’s all the Affirmative can do.

HARMS / SIGNIFICANCE

1. More study needed about the harms

Minority Report says “More Study.” Oversight board member says we need more study before deciding a policy

**Travis LeBlanc was a member of the Privacy & Civil Liberties Oversight Board that investigated and wrote a report on XKEYSCORE. The majority of that Board didn’t recommend abolishing XKEYSCORE, but what they did recommend is still classified. LeBlanc thought they weren’t critical enough and says they should have studied it more thoroughly. He doesn’t say he advocates the Affirmative position of abolishing it, but he says it needs more investigation to make an informed decision.**

Travis LeBlanc 2021 (former member of the Privacy & Civil Liberties Oversight Board) 12 March 2021 “Additional Unclassified Statement by Board Member Travis LeBlanc” commenting on the “Report on Certain NSA Uses of XKEYSCORE for Counterterrorism Purposes” <https://documents.pclob.gov/prod/Documents/Projects/4b4f65ff-0dba-444b-9c10-7e6b3fce407c/2021.06.28.Member%20LeBlanc%2012333%20Unclass%20Statement.pdf> (accessed 7 Feb 2022)



The majority report was a 6-year study of KEYSCORE. Its findings are classified, but we know they didn’t recommend abolishing KEYSCORE because Mr. Leblanc says they weren’t critical enough

NEW YORK TIMES 2021. “Privacy Watchdog Board’s Secret Report on N.S.A. System Fell Short, Member Says” 29 June 2021 <https://www.nytimes.com/2021/06/29/us/politics/nsa-xkeyscore-privacy.html> (accessed 7 Feb 2022)

The Privacy and Civil Liberties Oversight Board spent more than six years scrutinizing the surveillance-related system, called XKeyscore. Its report is classified.

COUNTERPLAN – Conduct more thorough study

XKEYSCORE may need reform, but the best qualified source – the Oversight Board – didn’t study it thoroughly enough

Travis LeBlanc 2021 (former member of the Privacy & Civil Liberties Oversight Board) 12 March 2021 “Additional Unclassified Statement by Board Member Travis LeBlanc” commenting on the “Report on Certain NSA Uses of XKEYSCORE for Counterterrorism Purposes” <https://documents.pclob.gov/prod/Documents/Projects/4b4f65ff-0dba-444b-9c10-7e6b3fce407c/2021.06.28.Member%20LeBlanc%2012333%20Unclass%20Statement.pdf> (accessed 7 Feb 2022)



Counterplan mandates

1. One month after a Negative ballot, the President will appoint with Senate confirmation a new 7-member XKEYSCORE oversight board chaired by Travis LeBlanc or anyone he recommends in his place who is acceptable to the President.

2. Board will investigate all the issues and gaps in the previous research identified by LeBlanc.
3. Board will issue a report no more than 3 years after a Negative ballot.
4. Congress will vote to accept the recommendations of the Board, which may be as follows: 1) No changes needed. 2) Reforms needed. Or 3) Abolish all of XKEYSCORE (the AI part and all the rest).
5. Funding from general federal revenues and cutting Dept. of Education Title 1 grants.
6. Enforcement by the President. Board members may be removed and replaced for malfeasance. The President will enforce the results of the Congressional vote when the results of the study are completed.
7. All Negative speeches may clarify.

Reasons to prefer the Counterplan

1. It’s non-topical and denies the resolution. We’re not “resolved” that any reform of AI is needed.

2. It’s mutually exclusive to the Affirmative plan. You can’t do their plan of immediately abolishing the AI part of XKEYSCORE and our “Wait and do more study” counterplan at the same time.
3. It relies on the best evidence. The majority report of the original oversight board didn’t recommend abolishing XKEYSCORE. The minority dissenters said we need to do a more thorough study before we decide what to do. Either way, the investigators who spent 6 years studying this are the best evidence in this round and they oppose the Affirmative plan.

4. We solve where Affirmative can’t. They can only reform the AI part of XKEYSCORE. We can reform or abolish the entire XKEYSCORE program if more study finds that to be the best policy.

2N / Rebuttal backup: XKeyScore

INHERENCY

Existing safeguards protect privacy

NSA uses multiple layers of safeguards to protect privacy and civil liberties

Morgan Marquis-Boire, Glenn Greenwald and Micah Lee 2015 (journalists) 1 July 2015 THE INTERCEPT “XKEYSCORE – NSA’s Google for the World’s Private Communications” <https://theintercept.com/2015/07/01/nsas-google-worlds-private-communications/> (accessed 7 Feb 2022)

In a statement to *The Intercept*, the NSA said:
“The National Security Agency’s foreign intelligence operations are 1) authorized by law; 2) subject to multiple layers of stringent internal and external oversight; and 3) conducted in a manner that is designed to protect privacy and civil liberties. As provided for by Presidential Policy Directive 28 (PPD-28), all persons, regardless of their nationality, have legitimate privacy interests in the handling of their personal information. NSA goes to great lengths to narrowly tailor and focus its signals intelligence operations on the collection of communications that are most likely to contain foreign intelligence or counterintelligence information.”

HARMS / SIGNIFICANCE

No evidence of harm specifically from AI + more study needed

The 6-year oversight board study never scrutinized the use of AI on XKEYSCORE

NEW YORK TIMES 2021. “Privacy Watchdog Board’s Secret Report on N.S.A. System Fell Short, Member Says” 29 June 2021 <https://www.nytimes.com/2021/06/29/us/politics/nsa-xkeyscore-privacy.html> (accessed 7 Feb 2022)

Mr. LeBlanc offered myriad criticisms of the report, portraying the board’s approval of it as rushed and pointing to gaps like a failure to scrutinize the use of artificial intelligence in connection with the system, to conduct an adequate assessment of oversight mechanisms, and to scrutinize the National Security Agency’s collection activities under Executive Order 12333, including those that can incidentally pull in Americans’ private messages.

Not enough study has been done on XKeyscore AI to know if it violates 4th Amendment privacy for US citizens

WASHINGTON POST 2021. “NSA surveillance program still raises privacy concerns years after exposure, member of privacy watchdog says” 29 June 2021 <https://www.washingtonpost.com/national-security/nsa-surveillance-xkeyscore-privacy/2021/06/29/b2134e7a-d685-11eb-a53a-3b5450fdca7a_story.html> (accessed 7 Feb 2022)

LeBlanc said the board did not analyze the extent to which XKeyscore’s use of machine analysis — as opposed to human review — of Americans’ information triggers Fourth Amendment scrutiny. The board, he said, ultimately “failed the public” by not using its investigation to “delve into important technological and modern electronic surveillance issues” raised by XKeyscore.

Reasons to prefer our evidence: Classified access is the best evidence

Mr LeBlanc had access to the classified information used by the oversight board, something none of the Affirmative’s sources had. If he says we don’t know enough about what XKEYSCORE is doing with AI, then nobody else really knows either.

Americans’ privacy not harmed

Questionable activities were actually just typos or minor mistakes, not systemic abuses

WASHINGTON POST 2021. “NSA surveillance program still raises privacy concerns years after exposure, member of privacy watchdog says” 29 June 2021 <https://www.washingtonpost.com/national-security/nsa-surveillance-xkeyscore-privacy/2021/06/29/b2134e7a-d685-11eb-a53a-3b5450fdca7a_story.html> (accessed 7 Feb 2022)

Rebecca Richards, NSA’s civil liberties and privacy officer, said: “When we looked at the [questionable intelligence activities] associated with this, we didn’t find any of them to identify systemic issues or any particular concerns. We found them to be standard intelligence practices.” The incidents could include making a typo in a query or making too broad a query, she said.

Privacy doesn’t matter anyway

Most people don’t care about privacy as much as they claim to

Prof. Neil Sahota 2020 ( IBM Master Inventor, United Nations Artificial Intelligence Advisor, Professor at UC Irvine) 14 Oct 2020 “Privacy Is Dead And Most People Really Don’t Care” https://www.forbes.com/sites/neilsahota/2020/10/14/privacy-is-dead-and-most-people-really-dont-care/?sh=5fc1aa97b733

Have you read the terms and conditions to use Facebook? Your smart phone? [Most people have not](https://www.npr.org/2014/09/01/345044359/why-do-we-blindly-sign-terms-of-service-agreements), and probably with good reason. They’re hundreds, if not, thousands of pages long. In fact, even contract lawyers with thirty years of experience have struggled in trying to understand these agreements. Deep down, though, each of us knows that we’re signing away our privacy rights to use these platforms and devices. So why do we do it? We don’t truly value privacy as much as we like to believe we do.

What people value is “security,” not privacy. Strong belief in data privacy is dead

Prof. Neil Sahota 2020 ( IBM Master Inventor, United Nations Artificial Intelligence Advisor, Professor at UC Irvine) 14 Oct 2020 “Privacy Is Dead And Most People Really Don’t Care” https://www.forbes.com/sites/neilsahota/2020/10/14/privacy-is-dead-and-most-people-really-dont-care/?sh=5fc1aa97b733

We already live in a world where people are used to sharing everything online. You know those phone phishing scams like the fraudsters pretending to be the IRS? [Young millennials and Generation Z fall victim](https://www.vice.com/en/article/pkedxy/millennials-and-gen-z-get-scammed-more-than-their-grandparents-sorry) to them the most of any generation because they’re used to giving information away. People get important value from these platforms and devices and accept the trade offs for it. Data security is still paramount, but the strong belief for data privacy is pretty much dead.

Naïve to expect privacy any more, and people’s behavior proves they don’t really care

Identity Management Institute 2019 (global certification organization dedicated to identity governance, risk management, and compliance) (article is undated but mentions events in Sept 2019) “6 REASONS WHY DATA PRIVACY IS DEAD” <https://identitymanagementinstitute.org/6-reasons-why-data-privacy-is-dead/> (accessed 27 Nov 2021)

Decreasing difference between private and identifiable data is recognized at the governmental level, which proves that expecting privacy is naïve. In its report published years ago, the Federal Trade Commission raised concerns about “the diminishing distinction” between de-identified and personally identifiable information. Therefore, the “death of privacy” goes far beyond conspiracy theories. Based on our observations of the latest incidents and trends, consumer privacy appears dead no matter how much consumers expect it or organizations, industry experts, and regulators try to ensure the confidentiality of personal information and reassure consumers that all their personal data is in good hands. As we observe the latest trends and news, we have a hard time reconciling consumer expectation of privacy with consumer behavior as they post so many personal information on social media.

COUNTERPLAN BACKUP

Sen. Wyden agrees: We need more information, we know far too little about it

WASHINGTON POST 2021. “NSA surveillance program still raises privacy concerns years after exposure, member of privacy watchdog says” 29 June 2021 <https://www.washingtonpost.com/national-security/nsa-surveillance-xkeyscore-privacy/2021/06/29/b2134e7a-d685-11eb-a53a-3b5450fdca7a_story.html> (accessed 7 Feb 2022)

“I continue to be concerned that Americans still know far too little about the government’s surveillance activities under EO 12333 and how it threatens their privacy,” said Sen. Ron Wyden (D-Ore.), a member of the Intelligence Committee, in a statement to The Washington Post. “I’ve been pressing for multiple PCLOB reports about EO 12333 to be declassified, which will shed light on these secret authorities that govern the collection and use of Americans’ personal information.”

Funding: $20 billion in extra money in the Title 1 Education budget this year

Secretary of Education Miguel Cardona 2021. “Statement by Secretary of Education Miguel Cardona on the President's Fiscal Year 2022 Budget 28 May 2021 <https://www.ed.gov/news/press-releases/statement-secretary-education-miguel-cardona-presidents-fiscal-year-2022-budget> (accessed 7 Feb 2022)

 The budget proposes a historic $36.5 billion investment in grants for Title I schools, a $20 billion increase from the 2021 enacted level.

SOLVENCY

1. Everyone else is doing it – you won’t get your privacy back

Lots of other agencies and governments are doing the same thing XKEYSCORE is doing

Bruce Schneier 2015. (internationally renowned security technologist, called a “security guru” by the Economist) 6 July 2015 “The Nuts and Bolts of XKEYSCORE” <https://www.lawfareblog.com/nuts-and-bolts-xkeyscore> (accessed 8 Feb 2022)

I always read these NSA documents with an assumption that other countries are doing the same thing. The NSA is [not made of magic](https://www.schneier.com/blog/archives/2014/05/the_nsa_is_not_.html), and XKEYSCORE is not some super-advanced NSA-only technology. It is the same sort of thing that every other country would use with its surveillance data. For example, Russia explicitly requires ISPs to install similar monitors as part of its [SORM](https://en.wikipedia.org/wiki/SORM) Internet surveillance system. As a home user, you can build your own XKEYSCORE using the public-domain [Bro Security Monitor](https://www.bro.org/index.html) and the related [Network Time Machine](https://www.bro.org/community/time-machine.html) attached to a back-end data-storage system. (Lawrence Berkeley National Laboratory uses this system to store three months' worth of Internet traffic for retrospective surveillance -- it used the data to [study Heartbleed](https://jhalderm.com/pub/papers/heartbleed-imc14.pdf).)

2. New Zealand

Link: New Zealand uses XKEYSCORE too

Bruce Schneier 2015. (internationally renowned security technologist, called a “security guru” by the Economist) 6 July 2015 “The Nuts and Bolts of XKEYSCORE” <https://www.lawfareblog.com/nuts-and-bolts-xkeyscore> (accessed 8 Feb 2022)

 For an example of how complex the searches can be, look at [this](http://media.nzherald.co.nz/webcontent/document/pdf/201513/WTO%20document.pdf) XKEYSCORE query [published](https://firstlook.org/theintercept/2015/03/22/new-zealand-gcsb-spying-wto-director-general/) [in](http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=11421370) March, showing how New Zealand used the system to spy on the World Trade Organization: automatically track any email body with any particular WTO-related content for the upcoming election.

Link: New Zealand shares intel with the U.S.

Lucy Craymer 2021 (journalist) 29 Apr 2021 “Five Eyes: What is it? And how has the intelligence group expanded into more of a diplomatic mission?” <https://www.stuff.co.nz/national/politics/124970043/five-eyes-what-is-it-and-how-has-the-intelligence-group-expanded-into-more-of-a-diplomatic-mission> (accessed 8 Feb 2022)

The alliance, officially known as the UKUSA Agreement, is a multilateral grouping that includes not only the United Kingdom and the United States but also Australia, New Zealand and Canada providing information sharing between the countries. The partnership began as an agreement between the UK and the US in 1946 that cemented the sharing of signals intelligence, or information elicited by intercepting communications between people. Information sharing had begun during World War Two as the countries joined forces to try to break Japanese and German codes. Canada joined in 1948. New Zealand and Australia became members in 1956.

Solvency Fail: The day after the AFF plan takes effect, the US government just asks New Zealand for all the same info

Affirmative has no jurisdiction over New Zealand, so they can’t stop them from using AI. And the Affirmative can’t abolish the US / New Zealand alliance.

3. Other NSA programs

NSA “MUSCULAR” program. It isn’t regulated by the AFF plan, so they’ll use that instead

Michael B Kelley, 2013 "The NSA Has Infiltrated The Clouds Of Both Yahoo And Google," October 30, 2013, Business Insider <https://www.businessinsider.com/nsa-infiltrated-both-yahoo-and-google-2013-10> (Accessed November 06, 2021)

The National Security Agency has secretly gained access to the main communications links connecting worldwide data centers of Yahoo and Google, Washington Post's Barton Gellman and Ashkan Soltani report. The Post, citing documents obtained from former NSA contractor Edward Snowden and interviews with knowledgeable officials, details a project called MUSCULAR that sends reams of customer data from hundreds of millions of user accounts, including those of Americans, to NSA servers.

4. Privacy is a problem too big to be solved

There’s nothing anyone can do about data privacy other than go back to the Stone Age

WALL STREET JOURNAL 2018 (Christopher Mims, technology columnist) 6 May 2018 “Privacy Is Dead. Here’s What Comes Next” <https://www.wsj.com/articles/privacy-is-dead-heres-what-comes-next-1525608001> (accessed 27 Nov 2021)

Short of living in a remote hut while forsaking cellphones, the internet and credit cards, there is no longer any way that you, as an individual, can prevent marketers, governments or malicious actors from gathering and using comprehensive, personally identifying information about you.