Tom Hanks Warns Fans Against Deepfake Advert Featuring His Likeness

Jordan Peele turns Obama into foul-mouthed fake-news PSA

How a deepfake Tom Cruise on TikTok turned into a very real AI company

Source: https://www.tiktok.com/@deeptomcruise

Source: https://youtu.be/cQ54GDmm1s0

Source: https://media-cldnry.s-nbcnews.com/image/upload/r/rockcms/2023-10/tom-hanks-ai-ad-me-2301001-c4189e.png

“Deeptomcruise”
Metaphysic.ai

Follow

3 Following 5.1M Followers 19.4M Likes

Parody and younger!

Source: https://www.tiktok.com/@deeptomcruise

“Tom Hanks Warns Fans Against Deepfake Advert Featuring His Likeness”
WHAT DOES PUBLIC DATA GENERALLY REFER TO?

- Information that’s available to everyone without restrictions
- Information that’s accessible to the public, but may have some limitations
- Private or sensitive information specific to an individual that may be accessible via public records
- I’m not sure
- None of the above
How These Data Types Are Different

**Open Data**
Information that's available to everyone without restrictions

**Public Data**
Information that's accessible to the public, but may have some limitations

**Personal Data**
Private or sensitive information specific to an individual that may be accessible via public records
# Examples of Your Public Data

<table>
<thead>
<tr>
<th><strong>Public Records</strong></th>
<th><strong>Educational Records</strong></th>
<th><strong>Professional Licenses</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Birth certificate, marriage license, divorce record, property ownership</td>
<td>School directory, yearbooks, awards and honors, athletic records</td>
<td>License required by law or regulation to practice a specific profession</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Published Works</strong></th>
<th><strong>Community Involvement</strong></th>
<th><strong>Social Media Content</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Articles, books, research papers, blog posts, newsletters</td>
<td>Volunteer work, board membership, fundraising and advocacy activities</td>
<td>Publicly shared profile, tweets, posts, reactions, photos, videos, followers</td>
</tr>
</tbody>
</table>
HOW IS YOUR PUBLIC DATA COLLECTED?

DATA SCRAPING (WEB/SOCIAL MEDIA)

Extraction of data from websites and webpages or social media platforms
Which are ethical uses of your public data obtained through web scraping?

- Data analysis for research
- Data harvesting for spam
- Enhancing public services
- Manipulative political campaigns
- Creating data-driven applications
- Identity theft through data aggregation
<table>
<thead>
<tr>
<th>ETHICAL</th>
<th>UNETHICAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal insights &amp; reputation management</td>
<td>Identity theft</td>
</tr>
<tr>
<td>Data control &amp; identity protection</td>
<td>Stalking, harassment, bullying</td>
</tr>
<tr>
<td>Data cleanup</td>
<td>Phishing &amp; spamming</td>
</tr>
<tr>
<td>Job search</td>
<td>Invasion of privacy</td>
</tr>
<tr>
<td>Research &amp; advocacy</td>
<td>Misinformation &amp; defamation</td>
</tr>
<tr>
<td>Educational opportunities</td>
<td>Unauthorized profiling</td>
</tr>
<tr>
<td></td>
<td>Violating Terms of Service</td>
</tr>
</tbody>
</table>
DATA SCRAPING (WEB/SOCIAL MEDIA)
Extraction of data from websites and webpages or social media platforms

DATA BROKERS & AGGREGATORS
Companies that aggregate and sell your public data collected from various sources

HOW IS YOUR PUBLIC DATA COLLECTED?
COMMON TYPES OF DATA BROKERS

- Financial Information
- Risk Mitigation
- Marketing & Advertising
- People Search
- Health Data
WILL YOU SELL YOUR PUBLIC DATA WILLINGLY?

- Yes
- No
- It depends on the data
Based on a survey conducted in 2021 by SimpleTexting of more than 1,000 Americans,

- **HOME ADDRESS**: $1,048.60
  - 14.5% of people say they would not sell their home address

- **FAMILY STATUS**: $837.10
  - 14.9% of people say they would not charge for their family status

- **HEALTH STATUS**: $788.50
  - 13.5% of people say they would not sell their health status

- **FULL LEGAL NAME**: $516.10
  - 9.7% of people say they would not sell their full legal name

- **PRODUCT CONSUMPTION HABITS**: $293.10
  - 6.7% of people say they would not sell information on their general product consumption habits
HOW IS YOUR PUBLIC DATA COLLECTED?

DATA SCRAPING (WEB/SOCIAL MEDIA)
Extraction of data from websites and webpages or social media platforms

DATA BROKERS & AGGREGATORS
Companies that aggregate and sell your public data collected from various sources

PUBLIC RECORDS SEARCHES
Search for and retrieve public records from government agencies and organizations
PUBLIC RECORDS WITHIN YOUR DETAILED REPORT

- Arrest records
- Birth, marriage, divorce and death records
- Business registrations and corporate filings
- Court records
- Driving records and traffic violations
- Immigration records
- Professional licenses
- Tax records
- Vehicle ownership records
- Voting records
- Weapons licenses
How is your public data collected?

Data Scraping (Web/Social Media)
Extraction of data from websites and webpages or social media platforms

Data Brokers & Aggregators
Companies that aggregate and sell your public data collected from various sources

Public Records Searches
Search for and retrieve public records from government agencies and organizations

Web Cookies & Tracking Tech
Collect data about your online behavior (e.g., browsing habits and interests) and interactions
IS “CONSENT” AN ILLUSION?

Not all cookie banners are created equal.

1. **Notice-only banner**
   
   Our website uses cookies
   
   Our website uses cookies to continuously improve your experience and display content geared to your interests. By using our website and services, you agree to our use of cookies.
   
   [Got it]

2. **Implied consent banner**
   
   Our website uses cookies
   
   Our website uses cookies to continuously improve your experience and display content geared to your interests. We assume your consent to the cookies if you continue to use the website like interacting with the website or directing to any other page on the website.
   
   [Accept] [Decline]

3. **Explicit consent banner**
   
   Our website uses cookies
   
   Our website uses cookies to continuously improve your experience and display content geared to your interests. By clicking the “Accept All” button, you consent to activate all the cookies or the “Decline All” button to reject all the cookies except essential cookies. You can also visit the “Manage Preference” to provide the controlled consent.
   
   [Accept All] [Decline All] [Manage Preference]
DIFFERENT FLAVORS OF COOKIES

THE GYM SHOES YOU LIKED IN OUR SURVEY ARE ON SALE.
- GREAT.

ZERO PARTY DATA

I HEAR YOU HAVE A NEW GYM MEMBERSHIP. NEED ANY SHOES?
- WAIT, WHAT?

SECOND PARTY DATA

THE GYM SHOES YOU BROWSED LAST YEAR ARE ON SALE.
- UM, OK.

FIRST PARTY DATA

MAYBE YOU WOULDN'T HAVE SKIPPED YOUR WORKOUT TODAY IF YOU HAD NEW SHOES.

THIRD PARTY DATA
FIRST-PARTY COOKIES

STRICTLY NECESSARY COOKIES
Essential for the website to function and for you to use its features

PREFERENCES / FUNCTIONALITY COOKIES
Allow a website to remember your preferences to personalize your experience

STATISTICS / PERFORMANCE COOKIES
Gather information about how you interact with a website to make it better

MARKETING COOKIES
Track your behavior across websites to deliver targeted advertisements
MORE COOKIES

PERSISTENT COOKIES
Long-lasting and stored on your device, even after browser is closed

SESSION COOKIES
Temporary data while navigating a website, and deleted when the browser is closed or session expires

ZOMBIE COOKIES
Persistent tracking cookie that is difficult to delete and can regenerate even after removal attempts
TRACKERS TRACKING YOU

- WEB BEACONS
- FINGERPRINTING
- IP-BASED GEOLOCATION
- REFERRER DATA
- REPLAYS / HEATMAPS
HOW IS YOUR PUBLIC DATA COLLECTED?

DATA SCRAPING (WEB/SOCIAL MEDIA)
Extraction of data from websites and webpages or social media platforms

DATA BROKERS & AGGREGATORS
Companies that aggregate and sell your public data collected from various sources

PUBLIC RECORDS SEARCHES
Search for and retrieve public records from government agencies and organizations

WEB COOKIES & TRACKING TECH
Collect data about your online behavior (e.g., browsing habits and interests) and interactions
THE DARK SIDE
<table>
<thead>
<tr>
<th>How can your public data be misused for evil?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bullying</strong></td>
</tr>
<tr>
<td><strong>Catfishing</strong></td>
</tr>
<tr>
<td><strong>Data mining and profiling</strong></td>
</tr>
<tr>
<td>• Invasive</td>
</tr>
<tr>
<td>• Personal data used without consent</td>
</tr>
<tr>
<td><strong>Discrimination and bias</strong></td>
</tr>
<tr>
<td><strong>Doxxing</strong></td>
</tr>
<tr>
<td><strong>Identity theft and fraud</strong></td>
</tr>
<tr>
<td><strong>Physical harm and harassment</strong></td>
</tr>
<tr>
<td><strong>Ransomware</strong></td>
</tr>
<tr>
<td><strong>Reputation damage</strong></td>
</tr>
<tr>
<td><strong>Social engineering attacks</strong></td>
</tr>
<tr>
<td>• Phishing</td>
</tr>
<tr>
<td>• Spear phishing</td>
</tr>
<tr>
<td>• Whaling</td>
</tr>
<tr>
<td>• Smishing</td>
</tr>
<tr>
<td>• Vishing</td>
</tr>
</tbody>
</table>
AI-POWERED DATA MISUSE

**AI-enhanced deception**
Crafting convincing scams (e.g., phishing)

**AI-aided impersonation**
Building comprehensive profiles

**Deepfakes**
- Manipulating images & videos to create

**AI-driven content**
Manipulate or generate fake reviews, comments, or social media posts

**AI-assisted manipulation**
Tailored attacks, manipulative personas

**AI for large-scale theft**
Target identification
Dear [Employee Name],

I hope this email finds you in good health and high spirits. I am writing to you today with a surprise that I believe will lift your spirits even higher.

As you may be aware, our company has been experiencing financial success of late. I am pleased to announce that this success has allowed us to grant our hard-working employees a pay raise. You, [Employee Name], are one of those employees.

Attached to this email, you will find a document detailing the specifics of your raise. Please review it at your earliest convenience and do not hesitate to reach out to me with any questions.

Your hard work and dedication to our company have not gone unnoticed, and I am thrilled to be able to recognize your contributions in this way.

Once again, congratulations on your pay raise. Keep up the great work.

Best regards,

[Your Name]
At the end of the day, it’s not going to matter to us if something was written by an AI or not. We still need to understand it for what it is, not for what wrote it.

— Andy Patel, Researcher, WithSecure
# Best Practices for Protecting Your Public Data

<table>
<thead>
<tr>
<th>Review Settings</th>
<th>Share Mindfully</th>
<th>Use Passphrases</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regularly review and adjust your privacy settings across browsers, apps, social media, etc.</td>
<td>Limit sharing and access to only what you would want to be publicly available</td>
<td>Turn your passwords into passphrases and enable two-factor authentication</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Apply Updates</th>
<th>Educate Yourself</th>
<th>Dispose Securely</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keep OS, software and apps up-to-date with the latest security releases</td>
<td>Stay informed about emerging threats and scams as well as developments in data privacy laws/legislation</td>
<td>Properly shred or destroy your data securely to prevent physical access to your data</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Secure Communications</th>
<th>Monitor Digital Footprint</th>
<th>Backup Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Be cautious with public Wi-Fi networks, use a VPN, and even secure messaging</td>
<td>Keep an eye on your online presence to see what information is publicly available about you</td>
<td>Perform regular data backups to safeguard your public data</td>
</tr>
</tbody>
</table>
THANK YOU!
Be proactive in managing your online presence and cautious about what data you share publicly!
RESOURCES

EFF | Privacy
• https://www.eff.org/issues/privacy

Opt-Out Guides
• https://joindeleteme.com/blog/opt-out-guides/
• https://privacyrights.org/data-brokers

Look for and remove personal information from Google
• https://support.google.com/accounts/answer/1228138?sjid=18039433385525856187-NA

The Scrap Value of a Hacked PC
• https://krebsonsecurity.com/2012/10/the-scrap-value-of-a-hacked-pc-revisited/
• https://krebsonsecurity.com/2013/06/the-value-of-a-hacked-email-account/
RESOURCES

How are Companies Using Your Social Media Data?

What Is your Personal Data Worth? A Survey
  • https://simpletexting.com/blog/personal-data-value/

Generative AI Could Revolutionize Email—for Hackers
  • https://www.wsj.com/articles/generative-ai-could-revolutionize-emailfor-hackers-5a8c725c

The Fight for Privacy for Hackers by Danielle Keats Citron