

Learning & Privacy in Online Search

Doug Leith

School of Computer Science & Statistics,
Trinity College Dublin

... Its full of little details of our lives, work, interests, plans

... Its full of little details of our lives, work, interests, plans

The screenshot displays a web browser window with a 'Library' tab. The browser's address bar shows a search query. The main content area is divided into several sections. On the left, there is a sidebar with navigation options: 'History', 'Today', 'Yesterday', 'Last 7 days', 'March', 'February', 'January', 'December 2017', 'Downloads', 'Tags', and 'All Bookmarks'. The 'History' section is currently selected, showing a list of recent visits. Each entry in the history list includes a date, a name, tags, and a location. The 'All Bookmarks' section is also expanded, showing a list of saved links. The browser interface includes a search bar at the top right and navigation buttons at the top left.

Name	Tags	Location
SFI-Grant-Budget-Policy_2016_July-urfi-updates.pdf		http://www.sfi.ie/funding/sfi-policies-and-guidance/budget-finance-relat...
1-SFI-Team-member-scales-amendments_January-2018_Fina...		http://www.sfi.ie/funding/sfi-policies-and-guidance/budget-finance-relat...
Budget/Finance Related Policies		http://www.sfi.ie/funding/sfi-policies-and-guidance/budget-finance-relat...
sfi student stipend 2017 - Google Search		https://www.google.ie/search?client=firefox-b-ab&cdcr=0&ei=Dl_GWtXq...
sfi student stipend - Google Search		https://www.google.ie/search?client=firefox-b-ab&cdcr=0&ei=Bl_GWtXq...
tcd sfi student stipend - Google Search		https://www.google.ie/search?client=firefox-b-ab&cdcr=0&ei=_J7GWS1J...
tcd sfi student rates - Google Search		https://www.google.ie/search?q=tcd+sfi+student+rates&ie=utf-8&oe=utf...
Transcripts from Blackboard - Google Drive		https://drive.google.com/drive/folders/180bJmfq25Q8uyqQyL9HhBq4d1...
tnet-lee		https://mc.manuscriptcentral.com/longRequesttnet-lee?0DOWNLOAD...
E-Mail		https://mc.manuscriptcentral.com/tnet-lee?PARAMS=xik_Y19ouQJ6o...
ScholarOne Manuscripts		https://mc.manuscriptcentral.com/tnet-lee?PARAMS=xik_Y19ouQJ6o...
PoPETS_2018_4-paper76.pdf		https://submit.petssymposium.org/2018_4/doc.php/PoPETS_2018_4-paper...
Search - PoPETS 2018.4		https://submit.petssymposium.org/2018_4/search.php?q=re%3Ame
Goretex pro women's jacket - IMC		https://www.irishmountaineeringclub.org/forums/topic/goretex-pro-wome...
info - IMC		https://www.irishmountaineeringclub.org/forums/forum/info/
Buy/Sell, Lost/Found - IMC		https://www.irishmountaineeringclub.org/forums/forum/buysell-lostfound/
Any advice for lake como lake garda or Arco? - IMC		https://www.irishmountaineeringclub.org/forums/topic/any-advice-for-lak...
Events, Trips, Partners - IMC		https://www.irishmountaineeringclub.org/forums/forum/events-trips-part...
IMC - Irish Mountaineering Club		https://www.irishmountaineeringclub.org/
Log in IMC — WordPress		https://www.irishmountaineeringclub.org/wp-login.php?redirect-to=https...
Why can't I open Inkscape in El Capitan? - Apple Community		https://discussions.apple.com/thread/7677493
Inkscape and Mac OS 10.11 El Capitan - InkscapeForum.com		http://www.inkscapeforum.com/viewtopic.php?t=18978
Inkscape broken mac el capitan - Google Search		https://www.google.ie/search?q=inkscape+broken+mac+el+capitan&ie=u...
5 Free Adobe Illustrator Alternatives for Vector Graphics		https://www.techtics.com/5-free-adobe-illustrator-alternatives-vector-g...
alternative to adobe illustrator mac os editing eps - Google Se...		https://www.google.ie/search?client=firefox-b-ab&cdcr=0&ei=OvLFWRPIA...
alternative to adobe illustrator mac os editing pdf - Google Sea...		https://www.google.ie/search?client=firefox-b-ab&cdcr=0&ei=sHFHWqgeA...
User Guide - Exporting - Vectr User Guide		https://vectr.com/user-guide/toolbar/exporting/
User Guide - File Menu - Vectr User Guide		https://vectr.com/user-guide/toolbar/file-menu/
User Guide - The Editor - Vectr User Guide		https://vectr.com/user-guide/editor-basics/
User Guide - Vectr - Free Vector Graphic Design Software		https://vectr.com/user-guide/
Vectr - Free Online Vector Graphics Editor		https://vectr.com/
What are the best alternatives to Adobe Illustrator on OS X? - ...		https://www.quora.com/What-are-the-best-alternatives-to-Adobe-Illust...
alternative to adobe illustrator mac os - Google Search		https://www.google.ie/search?client=firefox-b-ab&cdcr=0&ei=4OXFqXq...
Mac OS X Inkscape		https://inkscape.org/en/download/mac-os/

Name: Last 7 days

What About Privacy ? And Who Cares Anyway ?

- “I’ve nothing to hide”
- “More personalised search and ads helps me” ?

What About Privacy ? And Who Cares Anyway ?

- “I’ve nothing to hide”
- “More personalised search and ads helps me” ?
- Ignorance is bliss – unconcerned because unaware ?
- What if its your teacher who is looking at it ? Or your parents ?
- Analogy with smoking ?

Its Not Just About You

- Impact of privacy breaches on business reputation e.g.
 - Facebook share value¹ (Cambridge Analytica etc)
 - Google's usage of UK health data²
- Business to business leakage of information e.g.
 - Pre-patent due diligence searches
- Abuses e.g.
 - Getting the dirt on the political opposition
 - Chilling effect on debate, self-censorship (try talking to someone who has lived under an oppressive regime)
 - Wilful misunderstandings

¹E.g see "Facebook Suffers Worst-Ever Drop in Market Value", Wall Street Journal, July 26 2018

²E.g. see "Google given access to healthcare data of up to 1.6 million patients", Guardian 4 May 2016

Privacy

Privacy vs Security

- Privacy is not the same as security/crypto
 - Security → admission control, akin to a lock. Either have access or do not
 - Privacy → release information in return for a benefit. Expect a trade-off between amount of information released and amount of benefit received.
- Current approach to online information sharing is largely binary, however – all in or all out.
 - Of course, this is by design and intentional.
 - But is it really necessary for delivery of personalised services (separately from the third party market in our data) ?

Privacy

Importance of Verification

- Contracts cannot be enforced unless compliance (or otherwise) can be verified.
- Suppose a provider says it doesn't use data that it sees, or that it provides some sort of private service. How can we verify this claim ? If we can't then we can't detect non-compliance let alone enforce compliance.
- Profit motive may be helpful here, hopefully at least.
- Note that we can only hope to provide evidence of learning, cannot prove absence of learning.

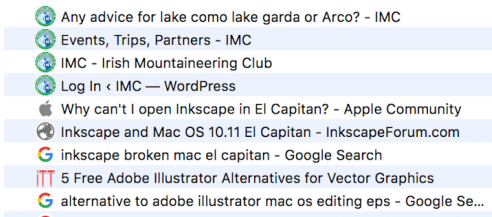
Online Search

Interface: Structured Interaction

Structured interface:

- Input queries
- Service responds with a results page
- User can click on links

We tend to enter sequences of related queries on a particular topic, then change topic and repeat. So interactions tend to consist of a set of sessions, each on a particular topic.



Online Search

Interface: Response Page

[All](#)
[Maps](#)
[News](#)
[Images](#)
[Video](#)
[Other](#)
[Settings](#)
[Instruments](#)

Approximately 2,180,000 results (0.48 seconds)

Hotel in Brescia | Easter Holidays Last Minute | booking.com
www.booking.com/brescia-hotel
 Evaluation for booking.com: 4.8 ★★★★★
 Book a Hotel in Brescia - Pay at the hotel without extra costs.
 We speak your language - Free cancellation - Best price guarantee - No additional costs
 Types: Hotels, Apartments, Villas, Hostels, Resorts, G & Bs

Book for tonight
Instant booking confirmation
24 hour customer support

Book for Tomorrow
Early and safe reservation!
New offers every day

112 Hotels in Brescia from € 44 | Your Ideal Hotel here | trivago.it
www.trivago.it/Hotels/Brescia
 Hotels in Brescia - Use trivago®: Hotels at Half Price, Compare Now!
 +1,300,000 Hotel - Compare - Find the Best Price - Hotel? trivago
 Services: WiFi, Swimming pool, Restaurant, Spa
 Hotel up to -78% - Hotel 4 Stars - Hotel Discounted Prices - 3-star hotel - Last Minute Offers
 Budget Hotels - up to € 90.00 / day - Compare and Save - Other *

Brescia Hotel | Hotels.com™ Official Website
www.hotels.com/brescia/hotel
 Evaluation for hotels.com: 4.4 ★★★★★
 Brescia Hotel Every 10 nights, you get 1 free!

Maximum price / night

€ 0 €

Sort by ▾ 2 ▾ Rating ▾ Type of accommodation ▾ Hotel category ▾

Services ▾

Hotel Fiera di Brescia
 3.4 ★★★★★ (241) - 4-star hotel
 Informa, WiFi and breakfast included
[GfGfGf](#) 23% discount

Al Ronchi Motor Hotel Brescia 4-star hotel near the...
 3.7 ★★★★★ (118) - 4-star hotel
 Low-key hotel with free parking
 Free Wi-Fi

€ 68
647

€ 51

10 Best Brescia Hotels (201 €) - TripAdvisor

<https://www.tripadvisor.it/Europe/Italy-Lombardy-Province-of-Brescia>
 Book the best hotels in Brescia on TripAdvisor - Find the best offer with 6,209 reviews and 2572 photos by travelers from 85 hotels in Brescia, Province of Brescia, Italy

The 30 best hotels in Brescia, Lombardy - Cheap hotels in Brescia

<https://www.booking.com/city/it/brescia.it.html>
 Fantastic discounts on hotels in Brescia, Italy. Good availability and competitive rates. Read the reviews and choose the right hotel for you.
 Guest house in Brescia - Bed & Breakfast in Brescia - Hotel Cristallo Brescia

The 30 best hotels & places to stay in Brescia, Italy - Brescia hotels

<https://www.getting.com/Italy-Lombardy> Translate this page
 Great savings on hotels in Brescia, Italy online. Good availability and great rates. Read hotel reviews and choose the best hotel deal for your stay.

Hotels in Brescia from € 27 / night - Search for hotels on KAYAK

<https://www.kayak.it/Hotels/Italy>
 Looking for a hotel in Brescia? 73-star hotel from 27 €, 3 stars from 33 € and 4 or more stars from 35 € and more at Novotel Brescia 2 from € 62 / per night, Hotel Ambassador from € 61 / per night, Una Hotel Brescia from € 45 / night. Compare prices for 114 hotels in Brescia on KAYAK.

Book your hotel in Brescia, Italy - Hotels.com

<https://it.hotels.com/Hotels-in-Italy>
 Book a hotel in Brescia - Choose the perfect accommodation from over 80 hotels in the city. Every 10 nights in the hotel you get 1 free *

Cheap hotel in Brescia starting from 35 € - Hotels.com

<https://it.hotels.com/Hotel-in-Italy/Brescia>
 Discover the 10 cheapest hotels in Brescia and book safely from € 35. Find your accommodation at the best price and save.

Online Search

Interface: Response Page

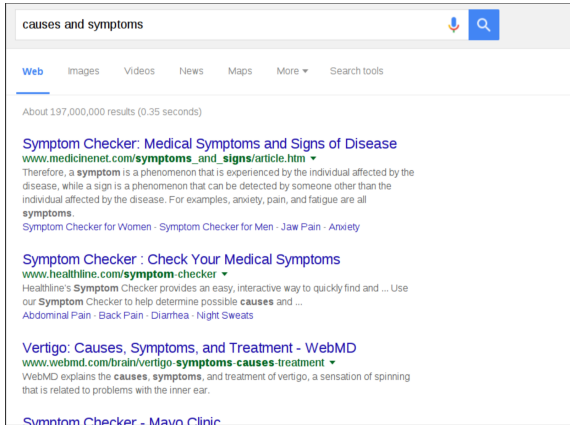
- Search results tend to be invariant ...
- ... but adverts are changeable.

Topic	Bing		Google	
	Advert	Link	Advert	Link
anorexia	65.4% \pm 7.7%	3.6% \pm 0.3%	34.8% \pm 1.5%	0.9% \pm 0.2%
bankrupt	15.8% \pm 1.5%	5.0% \pm 0.3%	39.0% \pm 2.5%	2.0% \pm 0.3%
diabetes	49.4% \pm 12.5%	3.9% \pm 0.3%	39.5% \pm 1.7%	0.9% \pm 0.2%
disabled	12.4% \pm 1.0%	3.5% \pm 0.2%	17.3% \pm 1.7%	2.1% \pm 0.3%
divorce	15.8% \pm 1.7%	4.7% \pm 0.4%	22.1% \pm 2.5%	2.9% \pm 0.5%
gambling	15.7% \pm 1.3%	4.0% \pm 0.2%	34.2% \pm 1.7%	1.8% \pm 0.3%
gay	13.8% \pm 1.3%	4.0% \pm 0.2%	34.3% \pm 1.8%	2.4% \pm 0.3%
location	16.3% \pm 1.5%	4.8% \pm 0.3%	25.3% \pm 2.1%	2.4% \pm 0.4%
payday	17.4% \pm 1.4%	3.9% \pm 0.2%	29.7% \pm 1.7%	1.4% \pm 0.3%
prostate	52.6% \pm 6.8%	3.7% \pm 0.3%	34.6% \pm 1.4%	0.9% \pm 0.2%
unemployed	14.3% \pm 1.2%	4.5% \pm 0.3%	22.8% \pm 1.8%	2.9% \pm 0.5%
other	17.8% \pm 27.9%	3.7% \pm 0.2%	27.5% \pm 1.5%	1.4% \pm 0.2%

Average percentage content change per instance of probe query, grouped by topic and search engine

- Can we exploit the responsiveness of adverts ? Remember for-profit organisations are obliged to maximise shareholder value. So if they think they know information about us that will do that ...

Online Search: Example of Using Probe Query



The screenshot shows a Google search interface with the query "causes and symptoms" entered in the search bar. The search results are displayed under the "Web" tab. The first result is from MedicineNet, titled "Symptom Checker: Medical Symptoms and Signs of Disease". The second result is from Healthline, titled "Symptom Checker : Check Your Medical Symptoms". The third result is from WebMD, titled "Vertigo: Causes, Symptoms, and Treatment". The fourth result is from Mayo Clinic, titled "Symptom Checker - Mayo Clinic".

causes and symptoms

Web Images Videos News Maps More Search tools

About 197,000,000 results (0.35 seconds)


Symptom Checker: Medical Symptoms and Signs of Disease
www.medicinenet.com/symptoms_and_signs/article.htm ▼
Therefore, a **symptom** is a phenomenon that is experienced by the individual affected by the disease, while a **sign** is a phenomenon that can be detected by someone other than the individual affected by the disease. For examples, anxiety, pain, and fatigue are all **symptoms**.
[Symptom Checker for Women](#) - [Symptom Checker for Men](#) - [Jaw Pain](#) - [Anxiety](#)

Symptom Checker : Check Your Medical Symptoms
www.healthline.com/symptom-checker ▼
Healthline's **Symptom** Checker provides an easy, interactive way to quickly find and ... Use our **Symptom** Checker to help determine possible **causes** and ...
[Abdominal Pain](#) - [Back Pain](#) - [Diarrhea](#) - [Night Sweats](#)

Vertigo: Causes, Symptoms, and Treatment - WebMD
www.webmd.com/brain/vertigo-symptoms-causes-treatment ▼
WebMD explains the **causes**, **symptoms**, and treatment of vertigo, a sensation of spinning that is related to problems with the inner ear.

Symptom Checker - Mayo Clinic

Online Search: Example of Using Probes Query



[Web](#) [Images](#) [News](#) [Videos](#) [More ▾](#) [Search tools](#)

About 136,000,000 results (0.46 seconds)

Blood sugar levels in diagnosing diabetes

Plasma glucose test	Normal	Prediabetes
Random	Below 11.1 mmol/l 200 mg/dl	N/A
Fasting	Below 6.1 mmol/l 108 mg/dl	6.1 to 6.9 mmol/l 108 to 125 mg/dl
2 hour post-prandial	Below 7.8 mmol/l 140 mg/dl	7.8 to 11.0 mmol/l 140 to 199 mg/dl

[1 more column](#)

Blood Sugar Level Ranges - Diabetes
www.diabetes.co.uk/diabetes_care/blood-sugar-level-ranges.html

Feedback

Ads

Diabetes Blood C
www.about.com/Diabetes Blood Chart.
Over 85 Million Visitors.

Diabetic Blood Te
www.zapmeta.com/Diabetic Blood Test
Find **Diabetic Blood Test** in 6 Search Engines at O

Blood Sugar Level
www.amazon.co.uk/low-prices-on-blood-sugar-level-ranges
Low Prices on **Blood Sugar Level Ranges**
Free Delivery on Orders

Change takes do
www.billionsinchange.com
See inventions that will change billions of lives, even you

Online Search: Example of Using Probe Query

causes and symptoms

Web Images Videos News Maps More Search tools

About 197,000,000 results (0.31 seconds)

Symptom Checker: Medical Symptoms and Signs of Disease
www.medicinenet.com/symptoms_and_signs/article.htm
Therefore, a **symptom** is a phenomenon that is experienced by the individual affected by the disease, while a **sign** is a phenomenon that can be detected by someone other than the individual affected by the disease. For examples, anxiety, pain, and fatigue are all **symptoms**.
Symptom Checker for Women - Symptom Checker for Men - Jaw Pain - Anxiety

Symptom Checker : Check Your Medical Symptoms
www.healthline.com/symptom-checker
Healthline's **Symptom** Checker provides an easy, interactive way to quickly find and ...
Use our **Symptom** Checker to help determine possible **causes** and ...
Abdominal Pain - Back Pain - Diarrhea - Night Sweats

Vertigo: Causes, Symptoms, and Treatment - WebMD
www.webmd.com/brain/vertigo-symptoms-causes-treatment
WebMD explains the **causes**, **symptoms**, and treatment of vertigo, a sensation of spinning that is related to problems with the inner ear.

Symptom Checker - Mayo Clinic
www.mayoclinic.org/symptom-checker/select-symptom/itt-20009075
Find possible **causes** of **symptoms** in children and adults. See our **Symptom** Checker.
Abdominal pain - Headaches - Dizziness - Low back pain

Symptom Of Diabetes
www.about.com/Symptom+Of+Diabetes
Search for **Symptom** Of Diabetes.
Find Expert Advice on About.com.

Diagnose your illness
www.whatsmydiagnosis.com/
Diagnose your **symptoms** accurately with an analytics diagnostic tool

Diagnose Me
www.diagnose-me.com/
Tell us about All your **symptoms**.
Let us give you the full picture.

Symptoms And Signs
www.amazon.co.uk/books
Save now on millions of titles.
Free Delivery on Orders over £25.

Symptoms Of Diseases
www.unitywalk.org/
Walk to Cure Parkinson's Disease!

- Looking for clear evidence of learning → confident in our inferences.
- If we query “diabetes” and see adverts related to diabetes, then that is weaker evidence that if we query “causes and symptoms” repeatedly and see diabetes adverts start to appear over time.

Details³

- **Training data T** . Consisting of displayed adverts tagged with a category e.g. sensitive/non-sensitive. Collect this data by a web crawl or logging adverts displayed to users via a browser extension.
- **Construct dictionary D**
 - Remove stop words e.g. a, of, the
 - Stemming e.g truncate {clicking, clicks, clicked} to click.
 - Assign unique integer id to resulting tokens from $T \rightarrow$ dictionary D
- **Vectorization of adverts**
 - Convert advert text to an integer vector x of size $|D|$ where value of x_w is the number of times token w appears in the advert (i.e. a “bag of words” model)

³Pol MacAonghusa, DL, *Don't Let Google Know I'm Lonely*, ACM Trans Privacy & Security 2016

Details

Example of Ad Vectorisation

Sky Bet Casino: Special Bonus | Receive a € 500 Bonus | skybet.it

[\(Ann.\) casino.skybet.it/benvenuto/bonus-casino](#) ▼

The best offers and the most beautiful games you find them only in our **casino** !

New Slots Every Month · Fast Recording · The thrill of the game Live · Unique gaming experience

Types: Slot Machine, Roulette, Black Jack, Poker

[Sign up now](#) · [Join Casino Now](#) · [Discover all the Slots](#)

[Soccer Betting](#) -up to € 150.00 - of Bonus · [Other](#) ▼

- Suppose dictionary $D = [\text{roulette, gam, casino, bet}]$
- “roulette” appears once in ad
- “gam” appears three times (“games”, “game”, “gaming” are all stemmed to “gam”).
- Vector associated with advert would be $x = [1, 3, 3, 2]$
- We do not include words not in dictionary D .
- Note that we can apply this process to create a vector associated with a single ad, to all of the adverts on a page etc

Details

- Using our labelled training data T ...
 - For each keyword calculate (i) what fraction of adverts on a particular topic c contain the keyword and (ii) what fraction of all adverts contain the keyword.
 - E.g. keyword “casino” might appear in 90% of online betting adverts but only in 5% of adverts overall. In which case its potentially a good indicator of the topic “gambling”.
- Given a new page with adverts ...
 - We need to give more weight to keywords that appear frequently in the page
 - PRI estimator:

$$\sum_{w \in D} \left(\frac{\text{fraction of topic } c \text{ adverts with keyword } w}{\text{fraction of all adverts with keyword } w} \times \text{fraction of } w \text{ on page} \right)$$

- Value ≈ 1 indicates no evidence of learning. Large or small values show evidence of learning – use threshold based on training data.

Detection Accuracy

- Measured data: 37,134 queries and responses collected over 28 days.
- Queries are associated with 12 topics:
 - 10 are associated with discrimination (health, disability, sexual orientation) or sensitive personal conditions (gambling addiction, financial problems)
 - 1 is location related
 - 1 consists of the top 50 queries from Google Trends.
- Sensitive topic keywords are taken from wikipedia and open directory project.
- Queries augmented with common words e.g. “fat” → why am i so fat”

Detection Accuracy

	Reference Topic										
	anorexia	bankrupt	diabetes	disabled	divorce	gambling	gay	location	payday	prostate	unemployed
True Detect	100%	100%	96%	100%	100%	100%	100%	99%	99%	99%	100%
True Other	96%	96%	92%	100%	100%	100%	100%	100%	100%	100%	100%
False Detect	4%	4%	8%	0%	0%	0%	0%	0%	0%	0%	0%
False Other	0%	0%	4%	0%	0%	0%	0%	1%	1%	1%	0%

Measured detection rate of google search learning of individual sensitive topics⁴

- True Detect = learning of topic detected, False Detect = mistake
- True Other = no evidence found of topic learning, False Other = mistake

⁴Pol MacAonghusa, DL, *Don't Let Google Know I'm Lonely*, ACM Trans Privacy & Security 2016

Speed of Learning By Search Engines

Number of Consecutive Misclassifications (X)			Probe ID of First Misclassification (Y)		
	Bing	Google		Bing	Google
$\mathbb{P}(X = 1)$	0.23	0.95	$\mathbb{P}(Y = 1)$	0.92	0.98
$\mathbb{P}(X = 2)$	0.77	0.05	$\mathbb{P}(Y = 2)$	0.03	0.01
$\mathbb{P}(X = 3)$	0.00	0.00	$\mathbb{P}(Y = 3)$	0.04	0.01
$\mathbb{P}(X = 4)$	0.00	0.00	$\mathbb{P}(Y = 4)$	0.00	0.00
$\mathbb{P}(X = 5)$	0.00	0.00	$\mathbb{P}(Y = 5)$	0.00	0.00

Probability of misclassification vs number of probes. $E[X|Google] = 1.05$,
 $E[X|Bing] = 1.77$

- Probes are sent on average every 4 queries, so Google appears to adapt to a new topic in approx 4 queries.

Logged In vs Anonymous

	Reference Topic										
	anorexia	bankrupt	diabetes	disabled	divorce	gambling	gay	location	payday	prostate	unemployed
True Detect	97%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
True Other	100%	100%	92%	100%	100%	100%	100%	100%	100%	100%	100%
False Detect	4%	0%	8%	0%	0%	0%	0%	0%	0%	0%	0%
False Other	3%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%

Measured detection rate of google search learning of individual sensitive topics when user is not logged in

Can We Slow Down/Disrupt Learning ?

Some ideas:

- Inject noisy queries into the user session (can be invisible to user if done in background via a browser extension). E.g.
 - Inject popular queries drawn from Google Trends
 - Be more sophisticated and try to mimic multiple user sessions
- User clicks can reveal user interests, so might also disrupt click behaviour. E.g.
 - Click nothing
 - Click all links
 - Click randomly selected links
 - Click links related to topics other than that of the user session

Do any of these strategies work ?

Plausible Deniability⁵

- Previous PRI detection approach estimates:

$$M_k(c) = \frac{P(\text{interest in topic } c | \text{user session up to } k\text{'th search})}{P(\text{interest in topic } c)}$$

- For a set of topics C and any pair of topics $c, d \in C$ for *plausible deniability* require:

$$e^{-\epsilon} \leq D_k(c, d) := \frac{P(\text{user session up to } k\text{'th search} \mid \text{interest in topic } c)}{P(\text{user session up to } k\text{'th search} \mid \text{interest in topic } d)} \leq e^{\epsilon}$$

- i.e. Require $|\log D_k(c, d)| \leq \epsilon$ for all c, d
- Using Bayes Rule:

$$D_k(c, d) = \frac{M_k(c)M_1(d)}{M_k(d)M_1(c)}$$

so can reuse PRI to estimate $D_k(c, d)$.

⁵Pol MacAonghusa, DL, *Plausible Deniability in Web Search*, IEEE Trans Inf Forensics & Security 2017

Measured Performance⁶

- Measured data: 21,861 queries and responses collected using same approach as before.
- For each test configuration responses for at least 2000 probe queries were collected, with 1000 used as training data and the other 1000 used for testing (with 7-fold cross-validation used to estimate sensitivity).

⁶Pol MacAonghusa, DL, *Plausible Deniability in Web Search*, IEEE Trans Inf Forensics & Security 2017

Measured Performance: Injecting Noise

Reference Topic	Probe 1	Probe 2	Probe 3	Probe 4	Probe 5
anorexia	48 (48)	48 (48)	48 (48)	48 (48)	48 (48)
bankrupt	16 (10)	65 (51)	65 (48)	65 (49)	65 (49)
diabetes	41 (38)	41 (38)	41 (38)	41 (38)	41 (38)
disabled	9 (9)	9 (9)	9 (5)	9 (7)	9 (8)
divorce	41 (27)	75 (38)	56 (22)	75 (29)	75 (29)
gambling	21 (16)	21 (3)	21 (4)	29 (16)	18 (4)
gay	86 (64)	86 (64)	80 (43)	94 (59)	94 (59)
location	10 (10)	8 (8)	8 (8)	18 (13)	18 (13)
payday	3 (2)	4 (2)	4 (2)	4 (2)	3 (1)
prostate	17 (15)	17 (15)	17 (15)	17 (15)	17 (15)
unemployed	10 (7)	13 (7)	13 (7)	13 (7)	13 (7)

Estimated $|\log D_k(c, d)|$ with no clicks and 3 random queries inserted after every user query. Reported as "Max (Median)" percentages⁷.

- $e^0 = 1$
- $e^{0.5} \approx 1.6$, $e^{-0.5} \approx 0.6$
- $e^{0.75} \approx 2.1$, $e^{-0.75} \approx 0.5$

⁷Pol MacAonghusa, DL, *Plausible Deniability in Web Search*, IEEE Trans Inf Forensics & Security 2017

Measured Performance: Random Clicks

Reference Topic	Probe 1	Probe 2	Probe 3	Probe 4	Probe 5
anorexia	50 (12)	27 (9)	26 (9)	36 (10)	33 (11)
bankrupt	5 (3)	43 (33)	39 (37)	36 (35)	38 (35)
diabetes	38 (6)	18 (7)	17 (5)	17 (7)	11 (5)
disabled	2 (1)	4 (1)	5 (3)	39 (25)	40 (25)
divorce	24 (17)	37 (31)	37 (31)	35 (25)	35 (25)
gambling	24 (0)	7 (4)	54 (23)	33 (23)	68 (20)
gay	68 (68)	68 (65)	54 (52)	46 (36)	47 (42)
location	8 (8)	8 (8)	8 (8)	8 (8)	8 (8)
payday	4 (1)	2 (2)	4 (2)	4 (3)	4 (4)
prostate	59 (57)	67 (62)	58 (56)	60 (54)	51 (44)
unemployed	4 (3)	8 (3)	10 (4)	3 (2)	10 (1)

Estimated $|\log D_k(c, d)|$ when click 2 links at random.

- $e^0 = 1$
- $e^{0.5} \approx 1.6$, $e^{-0.5} \approx 0.6$
- $e^{0.75} \approx 2.1$, $e^{-0.75} \approx 0.5$

Measured Performance: Clicking All

Reference Topic	Probe 1	Probe 2	Probe 3	Probe 4	Probe 5
anorexia	66 (57)	66 (57)	66 (57)	66 (57)	66 (57)
bankrupt	51 (42)	51 (42)	51 (42)	55 (46)	56 (46)
diabetes	35 (35)	35 (35)	35 (35)	35 (35)	35 (35)
disabled	9 (9)	9 (9)	9 (9)	31 (31)	31 (31)
divorce	30 (8)	73 (54)	54 (34)	100 (49)	100 (49)
gambling	3 (1)	16 (16)	53 (11)	16 (6)	6 (2)
gay	69 (65)	77 (73)	70 (60)	82 (75)	81 (71)
location	18 (10)	10 (6)	10 (6)	14 (10)	18 (7)
payday	2 (2)	2 (2)	2 (2)	2 (2)	2 (2)
prostate	17 (17)	17 (17)	17 (17)	17 (17)	17 (17)
unemployed	4 (4)	7 (7)	7 (7)	7 (7)	7 (6)

Estimated $|\log D_k(c, d)|$ when click all links.

- $e^0 = 1$
- $e^{0.5} \approx 1.6$, $e^{-0.5} \approx 0.6$
- $e^{0.75} \approx 2.1$, $e^{-0.75} \approx 0.5$

Measured Performance: Injecting Fake User Sessions

- Inject sequence of related queries. Topics used: tickets for events in Croke Park, vacation flights/hotels, car trade-in.
- Now have two interleaved sessions, the true user session and a fake one. Inject 3-4 fake queries for every true query, and randomly shuffle.

Reference Topic	Probe 1	Probe 2	Probe 3	Probe 4	Probe 5
all topics	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)

Estimated $|\log D_k(c, d)|$. Zero for all topics and all click strategies.

- $e^0 = 1$

Conclusions

- Its fairly straightforward to provide users with feedback on observed learning
- Learning by Google seems to fast, accurate and robust
- We can effectively disrupt this learning by injecting fake user sessions.
- But it seems like an arms race – personal queries are inherently revealing and we can expect use of more sophisticated learning approaches by the search engine to be able to extract them e.g. use of mixture models.
- Are there alternatives to this arms race ? Perhaps hiding in the crowd/clustering is an option – if were interested in personalised adverts, then we can likely get state of the art performance with much less personal information⁸.

⁸A.Checco, G.Bianchi, DL, *BLC: Private Matrix Factorization Recommenders via Automatic Group Learning*, ACM Trans Privacy & Security 2017