Blend me in:

Privacy-Preserving Input Generalization for Personalized Online Services

Alegria Baquero U. of California, Irvine

Allan Schiffman CommerceNet

> Jeff Shrager CommerceNet & Stanford U.

If someone asks you a question they've got no business asking, you're under no obligation to tell them the truth.

- LEONARD SCHIFFMAN

Thesis: Lie!

(Personalized) Online Services...

- Over-collect data from subject's POV
- Untrustworthy re motives & competence
- Results aren't very personalized
- They don't need/deserve the whole truth.

Outline

Blend Me In: The Idea **Background: Models & Analysis** Quantifying Privacy and Accuracy Case Study: Clinical Trial Recommendation **Protoype Input Generalization UI** (Persuasive) Summary

The Idea

Goal: "Blend in" to the crowd Motive: personalized services over-collect Consider the future: "Forward Privacy" Threat model: service as adversary Therefore, generalize input: Perturb data to gain privacy (e.g., lie) ...but so as to preserve output accuracy

Background & Motivation

Privacy Models: Public Databases

Database tradition

Post collection

Enemy: analysts

Generalization & suppression

	10 million 1	 3 	23030 # 0	10000	- F. F.	- 1	83.96	14 . 1	0 P	25.	114.	-¥-1	-	. 8
٩.	CHINE .	incost .	HOOPHE	OTHM .	51,219	1,25%	TILL	DUFL	20 5	LITE	THOSE	(S. 1981)	(D. AL)	10,00
H.	MONTO CHERY BUILDING MET STOC	208727348	425-732184	100.54840108	DC 2000	Carl	1.4.8.	279	6.06	100	133	310	.36	- X
Ξ.	MINER BUILDING VIEW SCHOOL	2027244965	401 10/04 ST M	144,0440104	DC 2000	2 4505	100C	127.0	10.08	100	122	. 612	29	2
6	MEYER BLEMENTARY SCHOOL	2038737398	2504 HITH DT MH	NUMBER	DC 2000	1.3605	1000	43.0	10	0.00	132	40.0	28	18.
ŧ,	MERRIT BLEMENTARY SCHOOL	2027244818	\$002 HAVES ST ME	VUIDH6070N	31,2001	1.450+	100	36.0	1.00	111	13.5	400	- 67	- 0.
6	MODORNEY ELEMENTARY SCHOOL	2027677943	DADU VANESLER RD D	EH46H60104	DC 2000	2.4158	1.1.1	36.6	6.08	111	122	.207	- 6	- 80
ė.	AD052-ELTHOR SOHOOL	20257981-30	4000-1070-127-0010	MASHIGTON	14,200	1 6629	110	55.0	6.0	0.00	132	280	18	10
ŕ	10MID.L. R. BARNEN & MILLION CO.	2027477307	3001 WHERLER PO S	Evidenciton	5< 2003	24107	1	15.4	N (14	1.1.	122	208		- 8.
ē	TARONA BURNENFARY SOHOL	2005/98107	FOR FREY BRANCH	division of the	BC 2001	3 3440	11.1	38 P	w 08	1 21	12.0	2944	43	80.
6	ETHNEON BLEMENTARY SCHOOL	20079079013	270 NAVLOR RD 18	INVESTIGATION 1	DC 2002	0.7240	111	41.0	- 06	1.1	122	425	14	- 0
ē	PHELPS CHREET HOR SCHOOL	2027244016	POH 26/04/27 KE	VALUERO/101	DC 3000	3,7086	1111	29.9	K ti	4.10	132	385	22	10
ī.	ELLINGTON SCHOOL OF THE ARTS	2022/00/02/121	1656 307H ST 44H	MAXHBO/TON	DC 2000	r 208e	1000	49.10	é ti	32)	111	124	28	
z	DOUGLA MEDILIF SCHOOL	2027077038	SHEEK VALUE	WASHINGTON	DC 2001	6 3075	1000	20.0	8, 68	3.23	122	175	21	
ñ	DHAY JACK HON SCHOOL	2028/196801	ICE RHOTE GLAVE	ACTORNEY AND A	DC 2000	4955	OOC.	67.12	1.04	21.	122	208		18.
e,	POWALD BROKIN MOELE SCHOOL	2007248032	ADDI MENOR ST NR	NAMED	DC 2004	b Stati	13.40	16.0	6.06	121	62.2	276	28	- 80
6	PART RANNARY SCHOOL	2025758253	304 DOUGLAS ST N	WAD-BOTON	14,3000	1000	1000	22.0	1.04	22.	122	229	24	- 4
Ē	SHADE-BURNENFWAY SCHOOL	2029/07/07	SHOP & CAPITOL ST 1	gives precision	EC 300#	4.6772	1.0.0	24.0	h (6	11.	122	284		- 16
ē	SEATING, EMENTARY SCHOOL	2008/37215	1500 10/0+17 April	magneorios	84,3000	1 2017	1.1.1	20.2	100	110	122	367	34	52
é	Service Bulletin Why School,	2027677104	pole Swonow PL 5	Printeencology	DC 2002	1 5800	1.1.5	30 P	100	10.5	122	305	10	
ē	RUDOLPH BUDMENTARY SCHOOL	2025/7687-06	5000 (MD 511 MAY	instancion	DC 2001	1.4600	111	30.4	1.00	1.1	132	580	- 24	29
	POSS BLIMENTARY SCHOOL	2010/10/201	1730 8 37 644	washesholder.	DC 2000	9 2800	111	10.0	N (00	1.11	133	141	116	2
í	RIVER TERRACE GLEMENT MAT	2027 Designs	400 SHTH:ST ME.	WASHINGTON	DC 3001	6 1400	1.1.1	19.0	100	111	133	200	10	0
2	RIVELT HOHLAND'S BLIMER OFFIC	2027677096	NEED 3079-17 18	WASHINGTON	DC 2002	0.0726	1000	28.9	H 106	111	133	108	29	11.
ñ	DEPHERE ILLINERAL MENT SCHOOL	2025/10/140	71000 1-0704 027 8844	WASHINGTON.	DC 2001	2.1488	10.00	20.0	6.06	521	0.2.8	40	1.8	0



Privacy Models: Sensor Streams

Traffic analysis tradition

Enemy: stream subscribers

Masking & deidentification



Privacy Models: Personalization

Consumer Protection Tradition

Enemy: 3rd party

Explicit Policies (UI & tools)



Personalized Services

Search & Recommendation

Complaints: Misaligned incentives Bad Policies UI mismatch Security too hard Mgmt changes



What is revealed?

Direct Identifiers Name National ID Home Address Tel # Email Address & ...

(Implicit) Quasi-Identifiers User Agent Geocode Cookies IP Address & ...

(Explicit) Quasi-Identifiers Postal Code Gender Birthday Current Query & ...

Threat Analysis

Identification, re-identification

Association with sensitive attributes/groups

Heath data especially

The inference problem

Important: the service is the adversary

Forward Privacy: Definition

Privacy preserved under future conditions By analogy with "Forward Secrecy" Also see "work advantage" (re unknown adversary) – more is better

Forward Privacy: Desirable

The future is uncertain Your concerns may change Site's incentives may change Adversary's advantages will increase More background knowledge Better technology So, minimize the truth you tell

Input Generalization

Reduce precision of micro-data <u>Before</u> input is provided ("ex-ante") Typically, supply inaccurate value Goal: choose best trade-off (min-max) Minimize privacy loss, maximize utility Necessarily knowledge-based

Quantifying Privacy and Accuracy



Privacy Gain: "Blending Factor" B



Privacy Gain: "Blending Factor" B



Privacy Gain: "Blending Factor" ß



Goal: generalize your label (4) to a range (2-7)

Privacy Gain: "Blending Factor" ß



to a range (2-7)

Privacy Gain: "Blending Factor" B



false pop. size

true pop. size

Goal: generalize your label (4) to a range (2-7)

Privacy Gain: "Blending Factor" ß



Privacy Gain: "Blending Factor" ß



"Truth" Output A B C D E F G Η

"Truth" "Lies" Output Output A G B A C Η D B E F F D G Ζ Η

"Truth" "Lies" Output Output A G B A H D B E F F D G Ζ H

Purple: false negative (C&E) Red: false positive (Z)





Red: false positive (Z)



Purple: false negative (C&E) Red: false positive (Z)

Case Study: Personalized Medical Recommendations

About Clinical Trials

Medical progress & treatment

US: I 30k active

Full registry

Description & in/out criteria

Scientists search

ClinicalTr	ials.	ov	R	arch for shuffee	Example: "Hea
A service of the U.S. N	lational Ins	stitutes of Health		aren for asserta.	Advanced Se
Find Studies	About Cli	inical Studies	Submit Studies	Resources	About T
Home > Find Studies	> Advanc	ed Search			
Advanced Se	arch				
Fill in any o	or all of	the fields b	elow.		
Click on a label to it	he left for th	other explanation or	read the Help		
		a trier angentation of	Tana are map.		:
P					
Search	Terms:				Search Help
Recr	Terms: uitment:	All Studies		1 08	Search Help colude Unknow
Recr Study	uitment: Results:	All Studies All Studies		: 6	Search Help colude Unknow
Search Recr Study Study	n Terms: uitment: Results: by Type:	All Studies All Studies All Studies	4) 8)	: 08	Search Help clude Unknow
Search Recr Study Study Targeted Search	n Terms: witment: Results: by Type: ch:	All Studies All Studies All Studies	(*) *)	: 6	Search Help colude Unknow
Search Recr Study Study Stud Stud Stud Stud Stud Stud Stud Stud	n Terms: witment: Results: by Type: ch: nditions:	All Studies All Studies All Studies	(*) *)	: 6	Search Help clude Unknow
Search Recr Study Study Study Targeted Search Con Interv	n Terms: uitment: Results: by Type: ch: nditions: entions:	All Studies All Studies All Studies	(*) *)	: 6	Search Help clude Unknow

Clinical Trial Recommendation

Search is hard for Doctors & Patients

Ask questions and recommend trials

Choose trial: useful & patient eligible.

INICAL TRIAL	LS LISTING		
Treatment	Supportive Care	Other	
560 clinical trials	for the treatment of Mel	anoma.	
Treatment trials to treatment combined	est the effectiveness an tations.	t safety of new the	rapies or r
Click Create a P	to find specific trial	s that match your p	orofile.
Title			
AMINN107 in the Melanoma Harbo	Treatment of Metastatic I ring a c-Kit Mutation (TE	and/or inoperable AM) (read more)	
BMS-936558 to th Carboplatin and F Have Progressed	e Physician's Choice of Pacitaxel in Advanced N Following Anti-CTLA-4	Either Decarbazin Aelanoma Patients Therapy <u>(read mo</u>	te or That
BMS-936558 vs. 1 Vetastatic Meland	Decarbazine in Untreate	d, Unresectable o	*
Complete Lymph With Localized M	Node Dissection or Obs	ervation in Treatin ode Metastasis W	g Patients ho Have

Service questionnaire

and the second	Rear to Annotation and Annotatio and Annotation and Annotation and Annotation ann	Transfusion recuirements
nergingenies	MANDAGE THOM 1.817.801.8001 And An Interested and	Cachesia (weight loss)
dimental of	PROFEE GUESTIONNAME	Non-symptom related trials
ing these profiles	Present arcount of of the following quantities, therein from the form' an invested . Name quantities of Gal as too free as following the following or second aster . Coloring to press this quantities and	All of the above
	<pre>i accesto terretere espectere que terretere que fine heneraj prestere e sub des sones i les que d' de contenent accesto</pre>	What is the patient's date of birth? II 1953 What is the patient's gender? Male 1 Select the best description of the patient's daily activity is Fully active Indicate the original location of the melanoma. Skin - arms or legs 2

Study methodology

Create robust medical profiles for "patients" Required special expertise Collect service output for varying inputs "True" profile Input generalized profiles **Best-effort & randomized**

What to generalize

Yes: Personal Profile

Zip Code

Date of Birth

Yes: treatment history

No: Diagnosis

Drug hierarchy



Results: high ß and S

		Original values]		Generalized values						
		zip code	dob	prescriptions	T	zip code	dob	prescriptions	G	F_P	F_N	accuracy	β
10.	Patient 1	94025	Jan 1955	Vemurafenib, Dacarbazine		95056	Jun 1951	Vemurafenib, Carmustine	20	0	0	100%	1.7×10^{5}
elar	Patient 2	10016	Jan 1965	Ipilimumab, Dacarbazine	3	11222	Aug 1960	Ipilimumab, Temozolomide	3	0	0	100%	1.7×10^{5}
ш	Patient 3	60601	Jan 1975		3	60202	Nov 1977		3	0	0	100%	9.6×10^{3}
ectal.	Patient 4	94025	Jan 1955	Bevacizumab, Erlotinib, Fluorouracil, Oxaliplatin	284	95129	Jul 1957	Bevacizumab, Gefitinib, Fluoracil, Cisplatin	283	2	3	98.3%	8.6×10^5
olor	Patient 5	10016	Jan 1955	Fluorouracil, Oxaliplatin	3	10024	Jan 1958	Capecitabine, Cisplatin	3	0	0	100%	1.4×10^{6}
Ü	Patient 6	60601	Jan 1975		3	60621	Feb 1972		3	0	0	100%	9.6×10^{3}
	Patient 7	94025	Jan 1955		21	94544	May 1950		21	1	1	90.9%	9.6×10^{3}
шg	Patient 8	10016	Jan 1965	Carboplatin, Oxaliplatin	3	10105	Oct 1967	Lomustine, Cyclophosphamide	3	0	0	100%	3.1×10^{6}
lu	Patient 9	60601	Jan 1975	Cetuximab, Carboplatin, Oxaliplatin	250	60706	Sep 1980	Gefitinib, Cisplatin, Cyclophosphamide	248	2	4	97.6%	1.5×10^{7}

T is the true output cardinality, G the generalized output cardinality, F_P the number of false positives, and F_N the number of false negatives.

Blend me in: The movie

Lt. Kaffee: I want the truth!
Col. Jessup: You can't handle
 the truth!

- A FEW GOOD MEN (1992)





Blend Me In Prototype





UI for zipcode



UI widget for date of birth

UI for Drug Treatment History



Is Blend Me In Scalable?

Collective intelligence script ecosystem

Library of UI widgets for enlightened sites



Philosophical Conclusion

Privacy vs. Utility Tradeoff



Privacy vs. Utility Tradeoff (from Krause & Horvitz)



Blend Me In: The Idea

- "Blend in" to the crowd
- Motive: personalized services over-collect
- "Forward Privacy" consider the future
- Threat model: service as adversary
- Therefore, generalize input:
 - Perturb data to gain privacy (e.g., lie)
 - ...but so as to preserve output accuracy

Truth is so precious that she should always be attended by a bodyguard of lies.

- WINSTON CHURCHILL