

June 2024 Meetup #1









Privacy Leaks Beyond The Class-Level



PRESENTER

Cat Easdon Senior Privacy Engineer

Protecting Personal Data

whoami

- Senior Privacy Engineer and TechEvangelist at Dynatrace
- *i* obsessed Brit based in Innsbruck
- Outside of work: research and tech policy, probably an excessive amount of trail running, hiking, skiing...
- Previously: hacking CPUs at TU Graz





Privacy leaks at the class-level

Example of privacy leaking "getter"

```
public class Leaking {
    private Counter leakedCounter;
```

```
/* Getter generated by Eclipse: */
public Counter getLeakedCounter() {
    return leakedCounter;
}
```

Notice how the "getter" generated by Eclipse simply returns a copy of the **reference** to the private attribute; giving the client access to modify the internal state of an object in the class directly.

Full source code: http://repositories.jacob-sparre.dk/privacy-leaks-examples/

・ロト・日本・日本・日本・日本・日本

Jacob Sparre Andersen Privacy Leaks in Java Classes

Privacy Leaks in Java Classes, Ada-Europe 2014, by Jacob Sparre Andersen: https://jacob-sparre.dk

Privacy leaks *beyond* the class level



Mapping Data Flows, SIPA - Columbia University: https://mappingdataflows.com

Outline

Motivation

- What does privacy mean?
- Why does it matter?
- Privacy at the code level
- Privacy at the infrastructure level
- Privacy by design and how to build it into the SDLC

What does privacy mean to you?

National Comprehensive Data Protection/Privacy Laws and Bills 2023



- Right to know, access, export
- Right to update (rectify)
- Right to delete ("be forgotten")
- Right to data portability
- Plus more...
 - Right to restriction of processing
 - Right not to be subject to automated decisionmaking, incl. profiling (GDPR)
 - Right to opt out of sensitive data processing (CPRA)





- Privacy isn't about hiding everything!
- Society runs on information flows, but these flows should be *context-appropriate*
- Data type, data subject, sender, recipient, legal basis, and purpose all matter



Why does privacy matter?

Privacy threats





Privacy Threat

Linkability

Identifiability

Non-Repudiation

Detectability

Data Disclosure

Unawareness, Unintervenability

Non-Compliance

Privacy Harms

Physical Harms

Economic Harms

Reputational Harms

Autonomy Harms

Psychological Harms

Discrimination Harms

Relationship Harms

Harm to the Business

Autonomy Harms

Coercion

Manipulation

Failure to Inform

Thwarted Expectations

Lack of Control

Chilling Effects

Privacy Harms, Citron & Solove, Boston University Law Review (2022)

Privacy harms: manipulation

 Neuroticism - Trapped
 Neuroticism - Stress Reactors
 Neuroticism - Self Lovers

 Neuroticism - Easily Deflated
 Neuroticism - Internal Escapists

 General Attitudes - I generally get a raw deal out of life
 Dealing with Stress - Hot and Cold

 Dealing with Stress - Emotional
 Dealing with Stress - Bottled Up

Clickagy > Health > Addictions > Alcohol







Skydeo > ConditionGraph > Disease Propensity by Type > **Depression** Diagnosis

VisualDNA Lifestyle - Lifestyle - Health - Trying to cut down on Alcohol Data provider: Nielsen Marketing Cloud

TransUnion - Demographics - Marital Status - Likely Recently Divorced

AlikeAudience: United States > Interest > Entertainment > Party And Night Club Enthusiasts

Eyeota - US Acxiom - CPG - Alcoholic Drinks - Vodka Brand - Grey Goose for age 21+ - Likely



Privacy at the code level

Privacy leaks at the class-level: an alternative perspective

```
final var response = startQueryForUser(user, tenantInfo).block();
final LocalDateTime retrievedAt = LocalDateTime.now(ZoneOffset.UTC);
if (response == null) {
    log.error("Request to tenant {} for user {} failed!",
        tenantInfo.url(), user.email());
    return new ResultAtTime<>(retrievedAt, result: null);
} else if (response.requestToken() != null) {
    // ...
```

```
"object": "user",
"id": "uuid-redacted",
"email": "a.sample.email@email.com",
"name": "Cat Easdon",
"picture": "https://lh3.googleusercontent.com/a/url-redacted",
"created": 1702548524,
"phone_number": "+431234567890",
"groups": {"object": "list"...}
```

Privacy in API design

Beyond the DTOs, also ensure that personal data is not included in endpoint paths:

privacy-rocks.com/settings/maria@email.com

privacy-rocks.com/confirmation?user=andreas@email.com&token=ab456d

Otherwise, this data may be stored in the browser history and server logs, and gets sent to:

Proxies and CDNs

• •••

- Google (or other ad vendor) and analytics providers
- Observability tooling

Privacy in observability tooling

🗊 Dynatrace			🍸 🕻 Last 2 hours
Q Search 🕱 K	Distributed traces		
🚱 Davis CoPilot 🛛 🕱 I	Browse and find distribute	d traces 🖸 in your environment.	
Apps			
Pinned	May 31	conversionRequest http://i.i.thtp://api.exchangeratesapi.io/v1/latest?access_kev=1234abcdefg&bas	se=U 107 µs - collector-trace-exporter ····
🍘 Notebooks			
🜃 Dashboards	Metadata		Attributes Stored (4) Blocked (0)
🔀 Workflows	Service	collector-trace-exporter	http.status_code 200
🔕 Hub	Trace ID	302bcf7c87173fb0eea7ceb38a6b43c7	http://api.exchangeratesapi.io/v1/latest?access_key=1234abcdefg&base=USD&sym
Eli Dashbaarda Classis	Span ID	3bdeb8be8eadde7e	bols=EUR
	Parent span ID	e12149eb6f263d45	http.method GET
🕕 Problems Classic	Span kind	Internal	span.kind Client
Recently opened	Instrumentation scope	currencyService	$\langle 1 \rangle$
Access Tokons	Instrumentation scope version	*	
To Access Tokens	Resource Attributes	Stored (4) Blocked (0)	Dynatrace Internal-use Attributes
🥣 Distributed Traces			
😰 Privacy Rights	telemetry.sdk.language	nodejs	dt.entity.service SERVICE-733E67C99E04C98E
	telemetry.sdk.version	0.13.0	< 1 >
	telemetruselle name	collector-trace-exporter	
	teremen y.suk.mame	openterentet y	
	Timings		
	Start time	May 31 17:26:21.067	
	End time	May 31 17:26:21.067	
	Response time	107 µs	

Privacy in sensitive contexts

				29.	ရ Ju	GRAZ Ini	20)2	4
	🗘 Inspect	or 🕥 Console (Debugger 🚺 Network {} Style Editor	Performance	ce :()î M	lemory	Storage ·	n Acc	cessibility 🎬 Application 🗇 🗇 🕶 🗙
Û 🗍	🗑 Filter URI	_s			H +	۹ ۵	All HTML	css	JS XHR Fonts Images Media WS Other 🗌 Disable Cache No Throttling 🖨 🔆
Status	Method	Domain	File	Initiator	Туре	Transferred	Size	Þ	Headers Cookies Request Response Timings Security
200	GET	🗎 www.csd-graz.at	et-divi-dynamic-tb-28-2-late.css	<u>/:45</u> (stylesheet)	CSS	2.48 kB	19.8	5	দ Filter Headers Block Resend
200	GET	www.youtube.c	SwNgfq2CrM4?feature=oembed	subdocument	html	39.52 kB	92		⑦ Host: www.youtube.com
200	GET	🔒 fonts.gstatic.c	memSYaGs126MiZpBA-UvWbX2vVnXBbObj2OVZ	font	woff	32.12 kB	31.2		Priority: u=4
200	GET	🔒 fonts.gstatic.c	memSYaGs126MiZpBA-UvWbX2vVnXBbObj2OV2	font	ttf	33.36 kB	51.1		(2) Referer: <u>https://www.csd-graz.at/</u>
200	GET	🔒 www.youtube.c	www-player.css	stylesheet	css	48.42 kB	376		Sec-Fetch-Dest: Iframe Sec-Fetch-Mode: pavinate
200	GET	🔒 fonts.gstatic.c	KFOmCnqEu92Fr1Mu4mxKKTU1Kg.woff2	font	woff2	11.56 kB	10.7		Sec-Fetch-Site: cross-site
-	0.57	<u>a.</u>			110	44.001.0	40.7		③ Sec-GPC: 1
0 1	118 request	s 12.02 MB / 5.80	MB transferred Finish: 4.80 min DOMConte	ntLoaded: 719 ms	load: 2.	.06 s		(⑦ Upgrade-Insecure-Requests: 1

Privacy in sensitive contexts

SVICIDE

When people feel hopeless and can't see any way to make things better, they sometimes want their life to end. But things can get better. There are people who can help.

If you feel suicidal and need help straight away, call 999 or call Childline on 0800 1111.

This page is also available in Welsh.

On this Page

Coping with how you feel Signs that someone may be suicidal Helping a friend who feels suicidal Losing someone to suicide

Status	Method	Domain	File
200	GET	A 🕅 cdn-ukwest.onetru	ot_guard_logo.svg
200	POST	🔒 jnn-pa.googleapis.com	Create
200	GET	🔒 www.youtube-nocooki	remote.js
200	GET	🔒 www.google.com	qPVc89Xtqb-imYcu3PoxhV
204	GET	🔒 www.youtube-nocooki	generate_204?YAmYDw
200	GET	🔒 www.youtube-nocooki	embed.js
200	GET	🔒 www.youtube-nocooki	www-embed-player.js
200	GET	🔒 www.youtube-nocooki	base.js

Privacy in sensitive contexts

In some contexts, every third-party request your web page or app makes may be an inappropriate flow of personal data!

Starting points:

- <meta name="referrer" content="noreferrer" />
- Don't include trackers (Google Analytics, Facebook Pixel / embedded social media or sharing links, videos...)
- Beware hidden tracking (e.g. Stripe)
- These are even easier to overlook when developing a mobile app!



Privacy at the infrastructure level

Privacy operations: rights at scale

How to keep track of personal data?

- Internal policies
- Code-level annotations
- Data and software catalogues
- Personal data detection and data-flow mapping



CCO Semgrep

public @interface MicrophoneAnnotation {
 String ID();
 Visibility[] visibility();
 MicrophoneDataType[] dataType();
 MicrophonePurpose[] purpose();
 String [] purposeDescription();
}

1	system:
2	- fides_key: demo_analytics_system
3	name: Demo Analytics System
4	description: A system used for analyzing customer behaviour.
5	system_type: Service
6	administrating_department: Engineering
7	egress:
8	– fides_key: another_demo_system
9	type: system
10	data_categories:
11	- user.contact
12	ingress:
13	<pre>- fides_key: yet_another_demo_system</pre>
14	type: system
15	data_categories:
16	- user.device.cookie_id
17	privacy_uectaracions:
18	data categories:
19	- user contact
20	- user device cookie id
21	data use: improve.system
22	data subjects:
23	- customer
24	egress:
25	<pre>- another_demo_system</pre>
26	ingress:
27	<pre>- yet_another_demo_system</pre>
20	

Privacy operations: rights at scale

- Once you've found the data, you then need to deal with incomplete exports or deletions due to:
 - Eventual consistency, caching, synchronization
 - Outages, timeouts
 - Immutable or "immutable in practice" data stores
 - Data warehousing and long-running data pipelines
 - Backups
- Two complementary approaches
 - Pseudonymize personal data -> centralize storage
 - Event-based pipelines
 - ...perhaps using Change Data Capture! ©



Source: <u>Imgflip</u>

Privacy operations: rights at scale

Deletion methods:

- API calls to each service (synchronous or async)
- Event-driven
- Offline / manual

Deletion needs to be *replayable* to handle:

- Outages
- Disaster recovery

Best if the team that owns each system also owns their role in export/deletion



Source: <u>Twitter Engineering</u>

Cross-border data transfers in the cloud



Privacy by design in the SDLC

Privacy by design

- 1. Proactive not reactive; preventative not remedial
- 2. Privacy as the default setting
- 3. Privacy embedded into design
- 4. Full functionality positive-sum, not zero-sum



Privacy by design

- 5. End-to-end security full lifecycle protection
- 6. Visibility and transparency keep it open
- 7. Respect for user privacy keep it usercentric



Security controls in the SDLC



agile process	Security workflows & automation, KPI monitoring, continuous improvement	aligned with
<u> </u>	Annual external penetration test, bug bounty program	ISO
bi-weekly sprints	Security trainings and security on-boarding program	27034-1

Privacy by design in the SDLC with privacy controls

- Threat modeling from initial design phase onwards
- Training and internal enablement
- Static code analysis
- Data and software cataloguing
- Privacy vulnerability handling
- Runtime scanning
 - PII detection
 - Data Loss Prevention (DLP)
- Privacy penetration testing and red-teaming







Thanks for listening!



