OPERANDO

Online Privacy Enforcement, Rights Assurance & Optimization

Constantinos Patsakis
University of Piraeus, Greece
OPERANDO

• Funded under the Horizon 2020 Programme (H2020), as part of the DS-01-2014 - Privacy call (GA no. 653704)

• We implement and validate an innovative privacy enforcement framework that will enable: Privacy as a Service

• The project is Open Source available in Github
Consortium
On 27 April 2016, the EU adopted new rules for the protection of personal data, via the **General Data Protection Regulation (GDPR)**. The GDPR will become applicable on **25 May 2018**, and its impact will be felt in many areas in the next few years that service providers will have to integrate it in their services.

- Will everyone do it?
- What happens till then?
- What happens with non-conforming services?
Main concept of the project

• **Ground truth**: Users do not have control of their private data.

• They consume numerous services, sharing their private data with many entities many of which they do not know.

• Users do not have control of **who** accesses their private data, **when**, **which** data and **why**.

• Users are not able to revoke their **consent**.

• Common users do not have the knowledge and means to enforce their privacy preferences.

• Note that the project was submitted before **GDPR**.
The OPERANDO approach

- “One size fits all” doesn’t actually work
- The project is split in G2C and B2C approaches to cater for the different needs.
- The research part of the project has several contributions that many of you are already using.
The G2C case
Current status

• Users browse the Internet sharing a lot of private information, without knowing what they share, when or being able to filter it.
• Big companies are monetizing this information as it enables them to efficiently profile users.
• Users have an “one-time” deal, “share data” or no-service.
• Many of the data that companies are collecting are not needed for the service provision.
How does it work? (User side)

• Users registered to a Privacy Service Provider (PSP) who provides them with a “vault” for their data
• Users then register to affiliated online service providers.
• The PSP provides an easy-to-use dashboard to manage all private data.
• The user can:
  • See which data each OSP requests,
  • Why they are requested,
  • When they are processed,
  • Who requests them
  • Revoke/grant access
OSP side

• The Online Service Provider (OSP) is not always the bad guy, actually most OSPs are not, they just want to provide a service.
• How do they prove that they “don’t do evil”?
• How can they get certification of their services?
• How they can deploy easily services?
OPERANDO PSP side

• OPERANDO provides the vault which is monitored by the PSP. All data coming, processed and leaving are continuously monitored and logged.

• To facilitate development all database transactions are made using a RESTful interface which allows developers to query the database using OData.

• Before executing any query, the role and permissions of each user are checked to determine whether he is authorized to perform the query. Then, the affected/returned rows are checked against the user preferences to determine whether user is allowed to perform this query in row level.
OPERANDO PSP side

• The PSP logs all transactions and shows you what is done with your data.
• The PSP monitors any transactions and enforces your privacy policies.
• The OSP cannot arbitrarily access your data.
• The OSP can handle user policies without writing any code.
• Opting in and out is seamless.
Basic concept of OPERANDO G2C
The AMI use case
Access preferences

PRIVACY SETTINGS FOR THE APP AMI

Your privacy preferences are shown here. You can see, and change, which organisations have access to your data and how it is used. These settings are enforced automatically for you by OPERANDO, an independent platform, to ensure that your data is only used in ways which you have agreed to.

Volunteer Link-Up should be able to access the following data:
- Data Metadata
- Id
- Availability
- Confidential Note
- Matches
- Preference
- Unsuccessful
- Volunteer Unsuccessful Reason
- Volunteer Checklist Items
- Email
- Title
- First Name
- Last Name
- Registration Date
- Address

Abingdon Good Neighbour Scheme should be able to access the following data:
- Data Metadata
- Id
- Availability
- Confidential Note
- Matches
- Preference
- Unsuccessful
- Volunteer Unsuccessful Reason
- Volunteer Checklist Items
- Email
- Title
- First Name
- Last Name
- Registration Date
- Address

Update APP User Privacy Policy Back to default values
**Mr North**

### Verification
- Registered
- Holds phone call
- Separate area
- Equivalent home
- Written references received
- PB2 informed
- Resided at least 3 months
- Successful exit

### Notes
- Please ensure all personal areas remain occupant's areas.

### Personal details

#### Address
- Suburb: 
- Street: 
- City: 
- Postcode: 
- Name: 

### Availability

<table>
<thead>
<tr>
<th>Available for week</th>
<th>Mon</th>
<th>Tue</th>
<th>Wed</th>
<th>Thu</th>
<th>Fri</th>
<th>Sat</th>
<th>Sun</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Distance travelled to work:
- 

### Preferences

<table>
<thead>
<tr>
<th>Accept</th>
<th>Construction</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Accept</th>
<th>Employment status</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Accept</th>
<th>Further support needed or is to full</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Accept</th>
<th>Depression</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Accept</th>
<th>Suicide, family history</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Accept</th>
<th>Plan to leave as an end</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Accept</th>
<th>Other issues or aspects</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>
Privacy Policy

AMI PRIVACY POLICY

Setting up your privacy policy will allow OPERANDO to enforce the statements within the policy. Since they are enforced, this information can be used to prove regulation compliance to regulators.

Who can use data

<table>
<thead>
<tr>
<th>User type of data user</th>
<th>User type of data subject</th>
<th>Type of information used</th>
<th>Reason for use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin Administrator</td>
<td>Volunteer</td>
<td>Email</td>
<td>Admin Newsletter</td>
</tr>
<tr>
<td>Volunteer Link-Up</td>
<td>Volunteer</td>
<td>Email</td>
<td>Arrange Interview</td>
</tr>
</tbody>
</table>

Notifications

Events relevant to you (e.g., pending data access requests, recommended automatic changes to settings) are displayed in this section. Requests are shown with the most recent first, but you can filter (Pending, Approved, Requested) or search freely.

NOTIFICATIONS

<table>
<thead>
<tr>
<th>Type</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin Privacy Policy change</td>
<td>Admin changed their Privacy Policy. Take a look at their Privacy Policy for details.</td>
</tr>
<tr>
<td>Admin Privacy Policy change</td>
<td>Admin changed their Privacy Policy. Take a look at their Privacy Policy for details.</td>
</tr>
<tr>
<td>Privacy Settings updated</td>
<td>Your privacy settings were updated because of changes you made through the dashboard.</td>
</tr>
<tr>
<td>Privacy Settings updated</td>
<td>Your privacy settings were updated because of changes you made through the dashboard.</td>
</tr>
<tr>
<td>Privacy Settings updated</td>
<td>Your privacy settings were updated because of changes you made through the dashboard.</td>
</tr>
</tbody>
</table>

Showing 1 to 5 of 5 records
**Privacy Policy**

**AMI PRIVACY POLICY**

From this page, you can see the privacy policies of the online services who can request your data. The policies are presented in a simple way (saying who using the service can view your data, what data they can see, and what it's used for), making the policy clear for everyone.

**Who can use data**

<table>
<thead>
<tr>
<th>User type of data user</th>
<th>User type of data subject</th>
<th>Type of information used</th>
<th>Reason for use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Volunteer Link-up</td>
<td>Volunteer</td>
<td>Email</td>
<td>Arrange Interview</td>
</tr>
<tr>
<td>Ami Administrator</td>
<td>Volunteer</td>
<td>Email</td>
<td>Ami Newsletter</td>
</tr>
</tbody>
</table>

---

**Reports (subscription and download)**

In this section you can manage your Reports: download available Reports, manage when reports are executed, or request a new Report definition is created.

- **Reports tab**: here you can find available Reports ordered by the most recently run first; click on a row to expand it and download. You can also search the Reports for certain words.
- **Schedules tab**: for each Report you can see the date of the last and next execution. Clicking on a row expands it, which allows you to view and manage the schedule for it. To add a new schedule, fill in the last row (with an orange background).

**REQUEST A NEW REPORT**

Show: 5

<table>
<thead>
<tr>
<th>Date</th>
<th>Report</th>
<th>Description</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>01/07/2017</td>
<td>Volunteer Breakdown Report</td>
<td>Breakdown of employment information and volunteering preferences</td>
<td>1.0</td>
</tr>
</tbody>
</table>

Showing 1 to 1 of 1 records
The B2C case
Consumer privacy is exposed to multiple dangers

DeFault Settings

• Times New Roman Syndrome – The default font for everything
• The users’ assumption that Online Service Providers had given careful consideration on their default privacy settings
• Privacy Settings not easily accessible to novice users

User Profiling

• Targeted Ads
• 3\textsuperscript{rd} party trackers
• Social media buttons

Unique identifiers to stalk users’ behavior

Keep in mind that using a free online service means that most probably you are the product.
Consumer privacy is exposed to multiple dangers

Forgotten & Suspicious Apps
• Remember that FB app you used once 2 years ago?
  – It still has access to your social network data
• Excessive permissions granted to mobile and browser apps

Email
• Spam emails after registration on websites
• Exposed after data breach of the Service Provider
  – e.g. Ashley Madison hack

Malware
• Malware software lurking on the internet
The complete guide to privacy


PlusPrivacy empowers users to

- Control all of social network privacy settings
- Ad blocking and anti-tracking capabilities
- Control the browser’s extensions permissions
- Control apps connected to their data
- Hide their email identity
- Do their own privacy-for-benefit deals

from a unified Dashboard
The users have to make only one choice.

Clicking the **Single click privacy** button will automatically change all the privacy options in your social network accounts to their most privacy-friendly settings.
Takes place on the browser, +P does not have access on users’ data.
Tweak your privacy settings from the dashboard
Ad Blocking

Anti-Tracking

Block Malware Domains
### Inspect the Permissions of Extensions

<table>
<thead>
<tr>
<th>Extension/App name</th>
<th>Intrusiveness</th>
<th>Enable/Disable</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Docs</td>
<td>1/10</td>
<td><img src="img" alt="Enable" /></td>
<td>perm_read</td>
</tr>
<tr>
<td>Gmail</td>
<td>6/10</td>
<td><img src="img" alt="Enable" /></td>
<td>perm_read</td>
</tr>
<tr>
<td>Google Docs Offline</td>
<td>5/10</td>
<td><img src="img" alt="Enable" /></td>
<td>perm_read</td>
</tr>
<tr>
<td>Google Drive</td>
<td>5/10</td>
<td><img src="img" alt="Enable" /></td>
<td>perm_read</td>
</tr>
<tr>
<td>{+P} Plus Privacy</td>
<td>7/10</td>
<td><img src="img" alt="Enable" /></td>
<td>perm_read</td>
</tr>
<tr>
<td>Sheets</td>
<td>1/10</td>
<td><img src="img" alt="Enable" /></td>
<td>perm_read</td>
</tr>
<tr>
<td>Slides</td>
<td>1/10</td>
<td><img src="img" alt="Enable" /></td>
<td>perm_read</td>
</tr>
<tr>
<td>YouTube</td>
<td>1/10</td>
<td><img src="img" alt="Enable" /></td>
<td>perm_read</td>
</tr>
</tbody>
</table>

#### Google Docs Offline permissions

- perm_read
- perm_write
- perm_identity
- perm_power
- perm_storage
- perm_unlimited_storage
- perm_webConnectable

#### Permission Warnings

- Communicate with cooperating websites
- Read and modify data you copy and paste
Just a click away from getting rid of redundant or privacy-polluting apps.

Inspect Apps connected to Facebook account:

<table>
<thead>
<tr>
<th>Logo</th>
<th>App name</th>
<th>Visibility</th>
<th>Permissions</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Developer</td>
<td>Friends</td>
<td>Public profile (required)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Friends list</td>
<td></td>
</tr>
<tr>
<td></td>
<td>MeetMe</td>
<td>Friends</td>
<td>Public profile (required)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Friends list</td>
<td></td>
</tr>
<tr>
<td></td>
<td>OpenChat Chat</td>
<td>Friends</td>
<td>Public profile (required)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Friends list</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Scribd</td>
<td>Friends</td>
<td>Public profile (required)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Friends list</td>
<td></td>
</tr>
</tbody>
</table>
Up to 20 alternative email identities

Remailed to your email address, and your reply will be mailed back to the original sender, without disclosing your real email address

+P does not keep any data
### PlusPrivacy

<table>
<thead>
<tr>
<th>Service provider</th>
<th>Deal</th>
<th>Reward</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://www.rafa.ro">www.rafa.ro</a></td>
<td>Valentine’s day</td>
<td>Get a 20% discount coupon</td>
</tr>
<tr>
<td><a href="http://www.rafa.ro">www.rafa.ro</a></td>
<td>Offer1</td>
<td>lorem ipsum</td>
</tr>
<tr>
<td><a href="http://www.rafa.ro">www.rafa.ro</a></td>
<td>2017 papers</td>
<td>Get 50% voucher when buying 2 papers and 30% for buying one paper</td>
</tr>
<tr>
<td><a href="http://www.rafa.ro">www.rafa.ro</a></td>
<td>Pigeon free</td>
<td>Discount for buying pigeons</td>
</tr>
<tr>
<td><a href="http://www.rafa.ro">www.rafa.ro</a></td>
<td>Music Festival</td>
<td>Free access</td>
</tr>
</tbody>
</table>

Allows users to get economic benefits in exchange for access to their private data (that today they provide for free!)
Easy to Use
User Interface
on Mobile Platforms
Research
You are already using our results

• A big part of our research is focused on improving S&P of Android and fixes have been already pushed.

• Android OS:
  • CVEs: 2017-0807 & 2016-6715
  • Unauthorized access to user’s location and user files.

• Apps:
  • Skype
  • Reported vulnerabilities to 20 of the most widely used medical apps
CVE-2017-0807 Detail

MODIFIED
This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Current Description
Source: MITRE  Last Modified: 10/02/2017  View Analysis Description

Impact

CVSS Severity (version 3.0):
CVSS v3 Base Score: 9.8 Critical
Impact Score: 5.9
Exploitability Score: 3.9

CVSS Severity (version 2.0):
CVSS v2 Base Score: 10.0 HIGH
Vector: (AV:N/AC:L/UC:N/C:C/I:C/A:C) (legend)
Impact Subscore: 10.0
Exploitability Subscore: 10.0
Contact us

Project webpage: https://www.operando.eu/
+Privacy has a dedicated web page: https://plusprivacy.com/

We share all our code on Github: https://github.com/OPERANDOH2020/

Social:
https://www.operando.eu/
https://twitter.com/OperandoH2020
https://www.facebook.com/OperandoH2020/