

# O{P}ERANDO

online privacy enforcement, rights assurance & optimization

## Taking Back Control of Your Data with OPERANDO

Achilleas Papageorgiou

Department of Informatics, University of Piraeus, Greece

INFOCOM 2017





# 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***

# Consortium



Fondazione  
**CENTRO SAN RAFFAELE**

# GDPR

- 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** 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**.

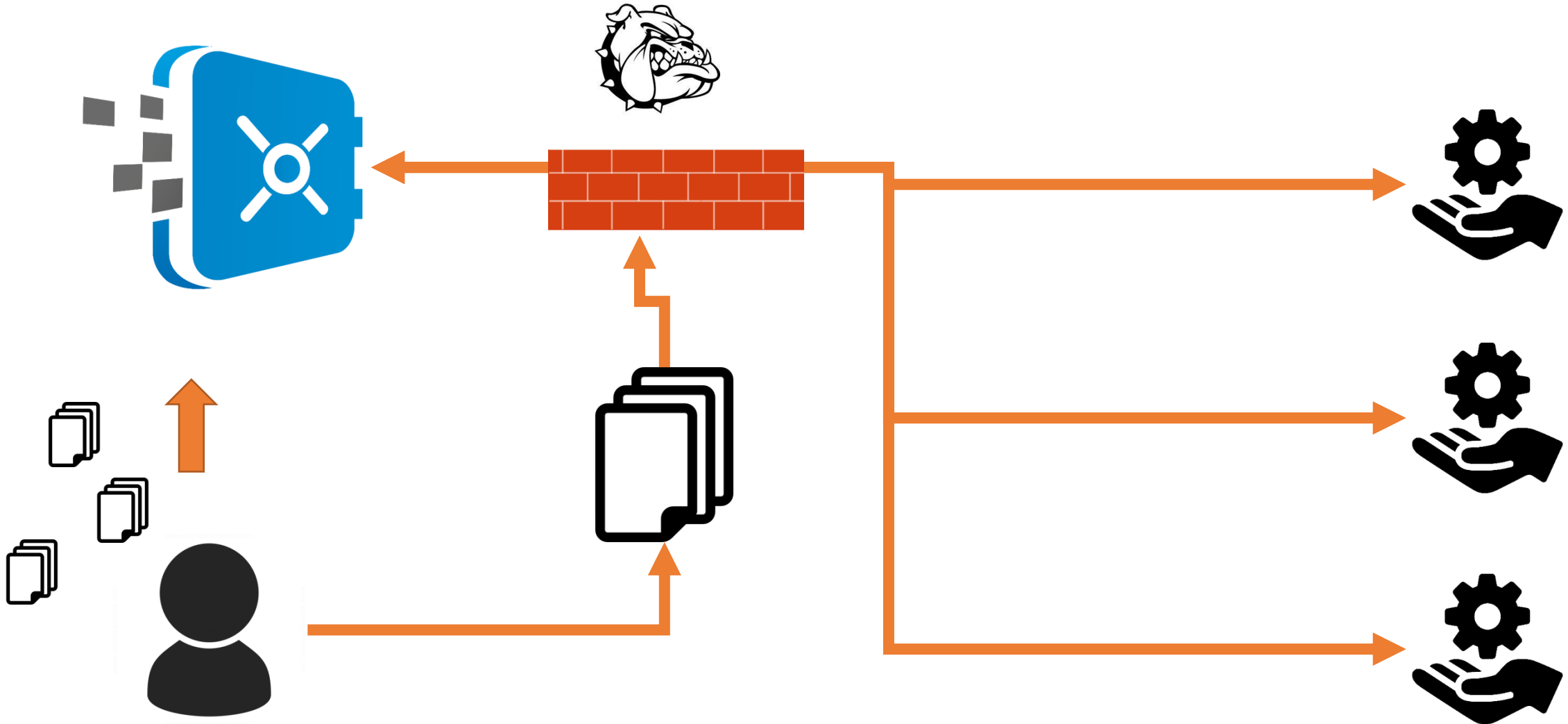
# The G2C case

# 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.



# Basic concept of OPERANDO G2C



# 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 services easily?

# 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.

# The AMI use case

[Dashboard](#)[Notifications](#)[Access Preferences](#)[Data Access Log](#)[Privacy Policy](#)

## 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:

- OData 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:

- OData Metadata
- Id
- Availability
- Confidential Note
- Matches
- Preference
- Unsuccessful
- Volunteer Unsuccessful Reason
- Volunteer Checklist Items
- Email
- Title
- First Name
- Last Name
- Registration Date
- Address

[Update UPP \(User Privacy Policy\)](#)[Back to default values](#)[Dashboard](#)[Notifications](#)[Access Preferences](#)[Data Access Log](#)[Privacy Policy](#)

## 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:

- OData 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:

- OData Metadata
- Id
- Availability
- Confidential Note
- Matches
- Preference
- Unsuccessful
- Volunteer Unsuccessful Reason
- Volunteer Checklist Items
- Email
- Title
- First Name
- Last Name
- Registration Date
- Address

[Update UPP \(User Privacy Policy\)](#)[Back to default values](#)

## Mr Robert North

## Verification

- Registered
- Initial phone call
- Interview arranged
- Successful interview
- References requested
- References received
- DBS complete
- Successful initial meeting
- Successful match

[End recruitment process](#)

S., T. Mr 60 y/o

Requested match

36 George Street, Oxford,  
Oxfordshire, OX1 2BJ (0.22 miles  
away)

Registration date: 28/06/2016

## Needs:

- Companionship (Top Need)
- GP appointment buddy

## Interests:

- History
- Music
- Sciences

[Edit match](#)

## Notes

These notes are confidential and cannot be seen by the volunteers.

## Personal details

Email address

bob@ami.com

Name

Mr

Robert

North

Registration date

17/10/2017

## Address

1 Oxford Road

Address line 2

Oxford

County

OX1 2EP

01234567890

## Availability

Available hours per week

2

Availability

	Mon	Tue	Wed	Thu	Fri	Sat	Sun
Morning	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Afternoon	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Evening	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Distance prepared to travel

5

Other

## Preferences

Occupation

Construction

Employment status

Fulltime employment

## Mr North

## Verification

- Registered
- Initial phone call
- Interview arranged
- Successful interview
- References requested
- References received
- DBS complete
- Successful initial meeting
- Successful match

[End recruitment process](#)

S., T. Mr 60 y/o

Requested match

36 George Street, Oxford,  
Oxfordshire, OX1 2BJ (7 miles  
away)

Registration date: 28/06/2016

## Needs:

- Companionship (Top Need)
- GP appointment buddy

## Interests:

- History
- Music
- Sciences

[Edit match](#)

## Notes

These notes are confidential and cannot be seen by the volunteers.

## Personal details

Email address

bob@ami.com

Name

Mr

First name

North

Registration date

17/10/2017

## Address

Address line 1

Address line 2

City or town

County

Postcode

Phone number

## Availability

Available hours per week

2

Availability

	Mon	Tue	Wed	Thu	Fri	Sat	Sun
Morning	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Afternoon	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Evening	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Distance prepared to travel

5

Other

## Preferences

Occupation

Construction

Employment status

Fulltime employment

Needs willing to fulfil

Companionship 

You can choose as many as you want

Hobbies and interests

DIY 

You can choose as many as you want



Dashboard

Notifications

Privacy Policy

User Policy Preferences

Big Data Analytics

Reports

## 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

User type of data user	User type of data subject	Type of information used	Reason for use	
Ami Administrator	Volunteer	Email	Ami Newsletter	<a href="#">Add +</a>
Volunteer Link-Up	Volunteer	Email	Arrange Interview	<a href="#">Edit</a> <a href="#">Delete</a>

Dashboard

Notifications

Access Preferences

Data Access Log

Privacy Policy

## 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






Show 5

Search: 

Type	Message
+ Ami Privacy Policy change	Ami changed their Privacy Policy. Take a look at their Privacy Policy for details.
+ Ami Privacy Policy change	Ami changed their Privacy Policy. Take a look at their Privacy Policy for details.
+ Privacy Settings updated	Your privacy settings were updated because of changes you made through the dashboard.
+ Privacy Settings updated	Your privacy settings were updated because of changes you made through the dashboard.
+ Privacy Settings updated	Your privacy settings were updated because of changes you made through the dashboard.

Showing 1 to 5 of 5 records

« &lt; 1 &gt; »

-  Dashboard
-  Notifications
-  Access Preferences
-  Data Access Log
-  Privacy Policy







## 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

User type of data user	User type of data subject	Type of information used	Reason for use
Volunteer Link-Up	Volunteer	Email	Arrange Interview
Ami Administrator	Volunteer	Email	Ami Newsletter

-  Dashboard
-  Notifications
-  Privacy Policy
-  User Policy Preferences
-  Big Data Analytics
-  Reports

## 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 with 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

[Request Now](#)

Reports Schedules

Show 5

Search:

Date	Report	Description	Version
01/07/2017 23:00:00	Volunteer Breakdown Report	Breakdown of employment information and volunteering preferences	1.0

Showing 1 to 1 of 1 records

« < 1 > »

# The B2C case

# OPERANDO B2C

- OPERANDO has a dedicated web page for B2C: <https://plusprivacy.com/>
- We have created **open source** software (available on Github: <https://github.com/OPERANDOH2020/PlusPrivacy>) to tackle with specific privacy issues
- We provide a Chrome extension, an Android and iOS app.
- **Goals:**
  - Privacy in Social Networks
  - Extensions and app management
  - Hide email identity
  - Ad blocking
  - Privacy-for-benefit deals

# Privacy in Social Networks

- Unified social networks privacy dashboard – allows you to choose the privacy settings for all your social networks from a single dashboard. There is also a “**single-click privacy**” **button** that automatically sets the privacy settings of all your SN accounts to their most privacy-friendly values. Currently Facebook, Twitter and LinkedIn are supported, with more SNs to be supported in the future.
- We inject JS code to perform these tasks for you so ***we never get hold of your credentials.***

# Extensions and app management

- ***Unified extensions and apps dashboard*** – allows you to review the extent to which each of the Chrome extensions and web apps connected to your Facebook, Twitter and LinkedIn accounts infringes on your privacy, and to take ***single-click disable/uninstall actions*** for such extensions/apps, without digging into the account settings of Facebook, LinkedIn, Twitter and Chrome.

# Hide your email identity

- We allow you to **generate** and use **up to 20 alternative email identities** in conjunction with your regular email service. Emails sent to your alternative identities will be automatically remailed to your email address, and you reply will be remailed back to the original sender, without disclosing your real email address.
- A remailer service allows this functionality, **we don't keep any data.**










# Ad blocking

- Largely based on Adblock Plus code, *without the “Acceptable Ads”*.
- All ads and trackers are blocked until explicitly whitelisted by the user.



# Privacy-for-benefit deals

- The Privacy-for-Benefit services will create business models based on consent of consumers to partially trade their private data for economic benefits from the participating online service providers. Under no circumstances will +P provide to 3rd parties any data of its users except based on their explicit opt-in.

Service provider		Deal	Reward		
	<a href="http://www.rafa.ro">www.rafa.ro</a>	Valentine's day	Get a 20% discount coupon		<input checked="" type="checkbox"/> Subscribe
	<a href="http://www.rafa.ro">www.rafa.ro</a>	Offer1	lorem ipsum		<input checked="" type="checkbox"/> Subscribe
	<a href="http://www.rafa.ro">www.rafa.ro</a>	2017 papers	Get 50% voucher when buying 2 papers and 30% for buying one paper		<input checked="" type="checkbox"/> Subscribe
	<a href="http://www.rafa.ro">www.rafa.ro</a>	Pigeon free	Discount for buying pigeons		<input type="checkbox"/> Subscribe
	<a href="http://www.rafa.ro">www.rafa.ro</a>	Music Festival	Free access		<input checked="" type="checkbox"/> Subscribe

# Participation is the key for success

- We are an open source project
- Github: <https://github.com/OPERANDOH2020/PlusPrivacy>
- You are more than welcome to join our platform and evaluate our services
- Let's take back the control of our data!
- URL: [www.operando.eu](http://www.operando.eu)

# Any questions?

## Contact info:

**Achilleas Papageorgiou, PhD Candidate, University of Piraeus**

**Email(s):** [achipapa@unipi.gr](mailto:achipapa@unipi.gr), [apapageorgiou@ieee.org](mailto:apapageorgiou@ieee.org)