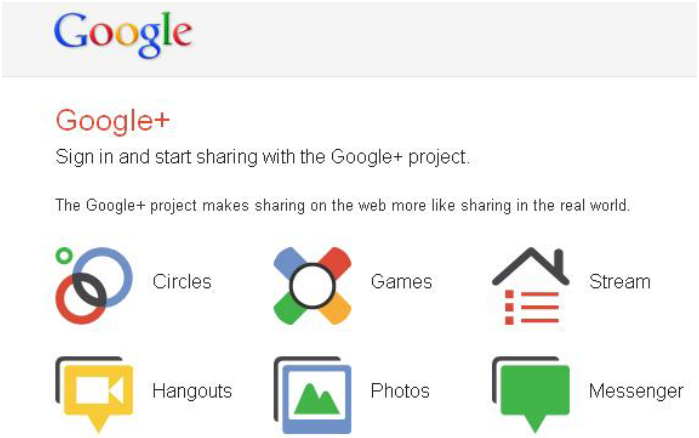
Towards Privacy-Preserving Communication Protocols for OSNs

Qiang Tang
q.tang@utwente.nl
DIES, University of Twente, the Netherlands

Outline

- Issues with Online Social Networks
- Introduction to the PPCP Project
- Acknowledgement

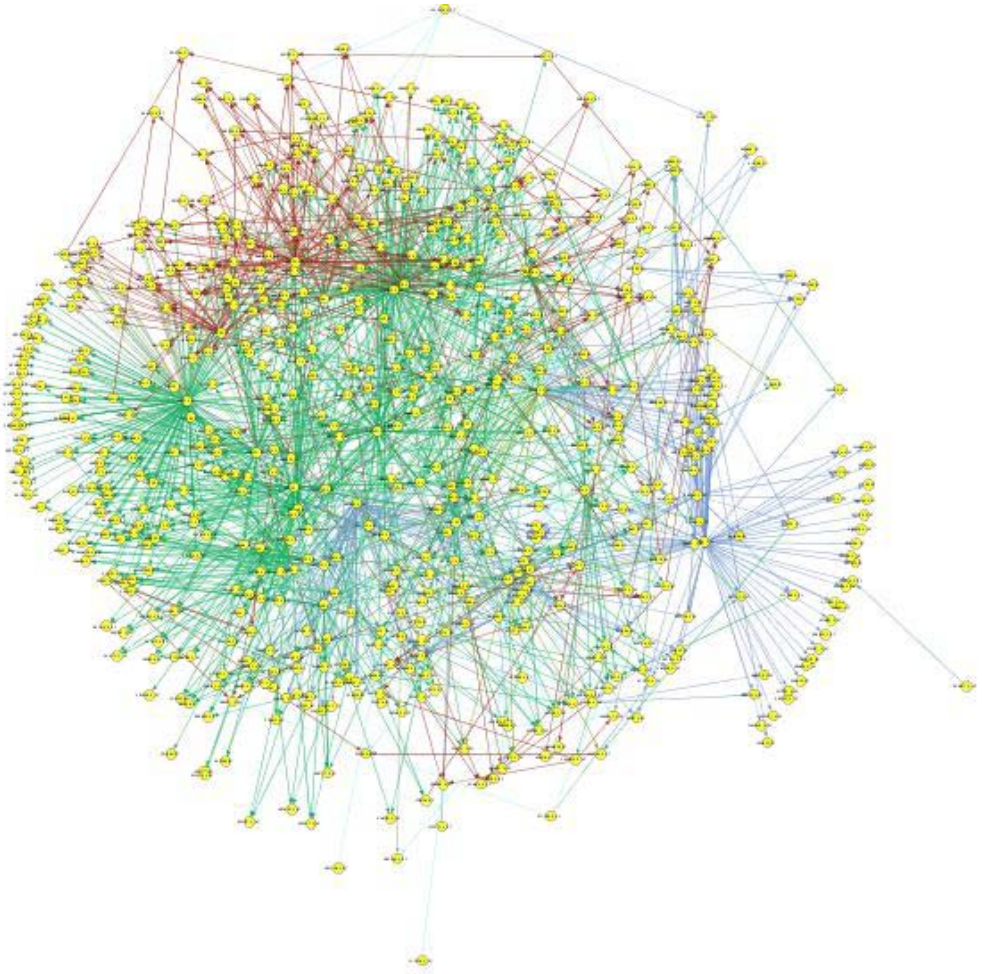
Online Social Networks are Everywhere



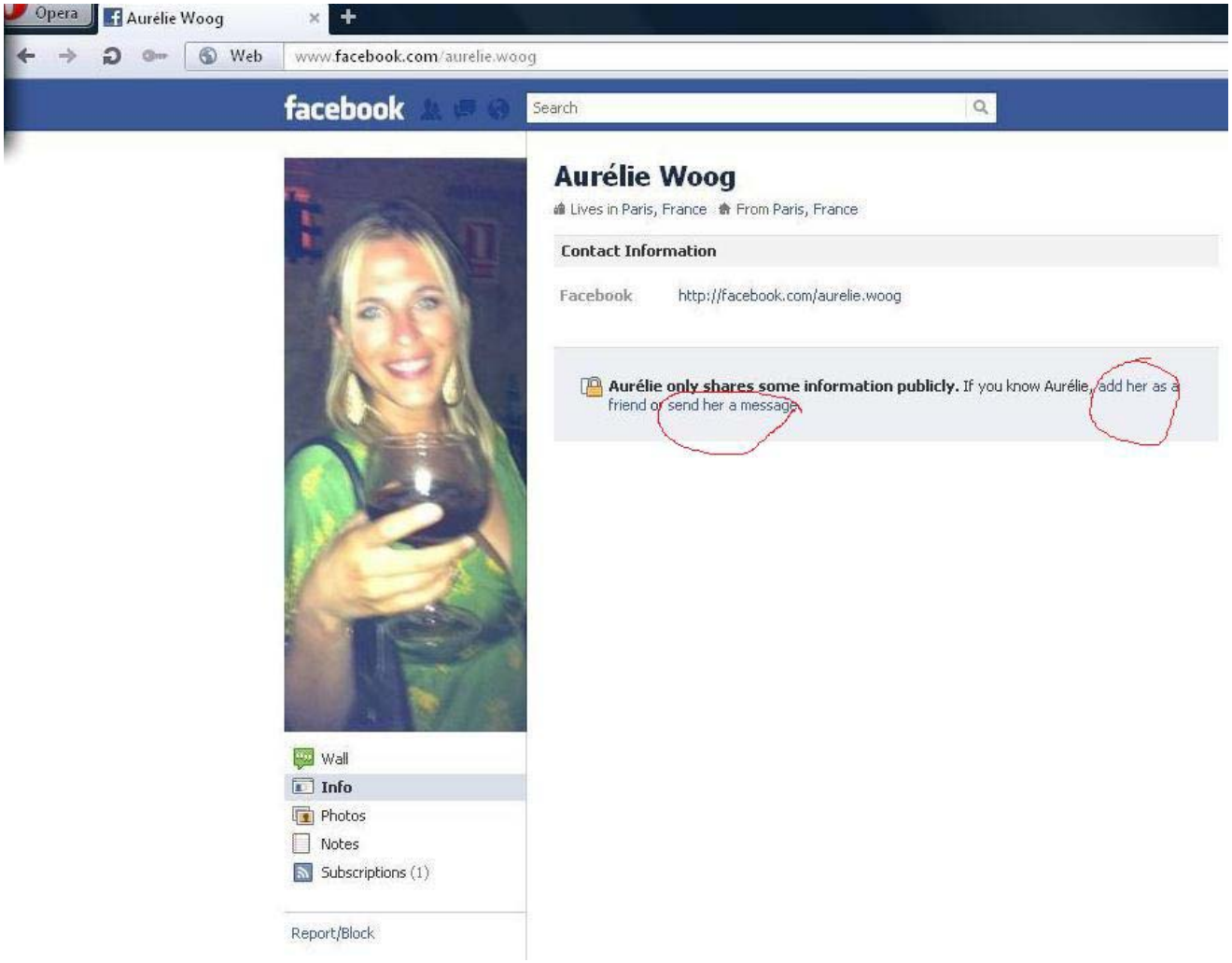
LinkedIn

New Communication Platform

- Social links exist intra & inter OSNs
  - Six degrees of separation theorem
- Extensive information sharing
  - Professional
  - Personal
  - Medical
  - …



Not Everything is Perfect



Privacy, Privacy, and Privacy

- OSNs know everything
- Third-party application could know everything
- Other agencies could know everything.

Home / News & Blogs / iGeneration

Microsoft admits Patriot Act can access EU-based cloud data

By Zack Whittaker | June 28, 2011, 8:10am PDT

Summary: *Microsoft's UK head admitted today that no cloud data is safe from the Patriot Act — and Microsoft will hand it over to U.S. authorities.*

LONDON — At the Office 365 launch, Gordon Frazer, managing director of Microsoft UK, gave the first admission that cloud data — regardless of where it is in the world — is not protected against the USA PATRIOT Act.

It was honestly music to my ears. After a year of researching the Patriot Act's breadth and ability to access data held within protected EU boundaries, Microsoft finally and openly admitted it.

The question put forward:

> "Can Microsoft guarantee that EU-stored data, held in EU based datacenters, will not leave the European Economic Area under any circumstances — even under a request by the Patriot Act?"

Frazer explained that, as Microsoft is a U.S.-headquartered company, it has to comply with local laws (the United States, as well as any other location where one of its subsidiary companies is based).

Though he said that "customers would be informed wherever possible", he could not provide a guarantee that they would be informed — if a gagging order, injunction or U.S. National Security Letter permits it.

He said: "**Microsoft cannot provide those guarantees. Neither can any other company**".

While it has been suspected for some time, this is the first time Microsoft, or any other company, has given this answer.

Trust is Hard to Establish

"On the Internet, nobody knows you're a dog."

Outline

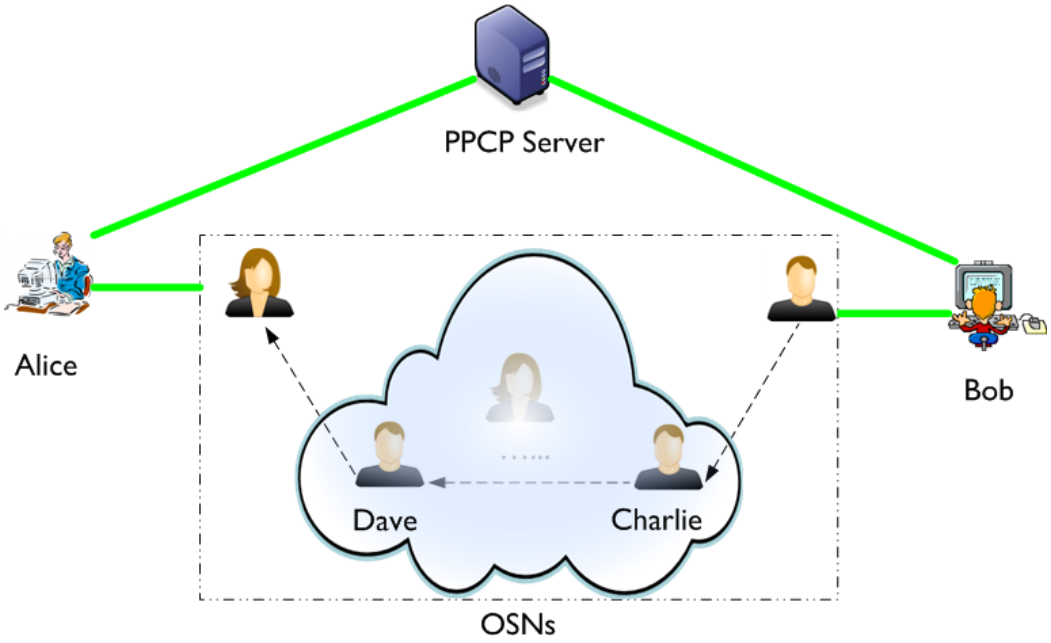
- Issues with Social Networks
- Introduction to the PPCP Project
- Acknowledgement

What is PPCP about?

- PPCP – Privacy Preserving Communication Protocols for OSNs
  - Enable users to store private profile attributes locally (without revealing to OSNs)
  - Enable two non-friend users to match their profiles, in an attempt to establish some sort of friendship
  - Enable two friend users to establish a secure channel and communicate with each other
- **It is an application complementary to existing OSNs.**

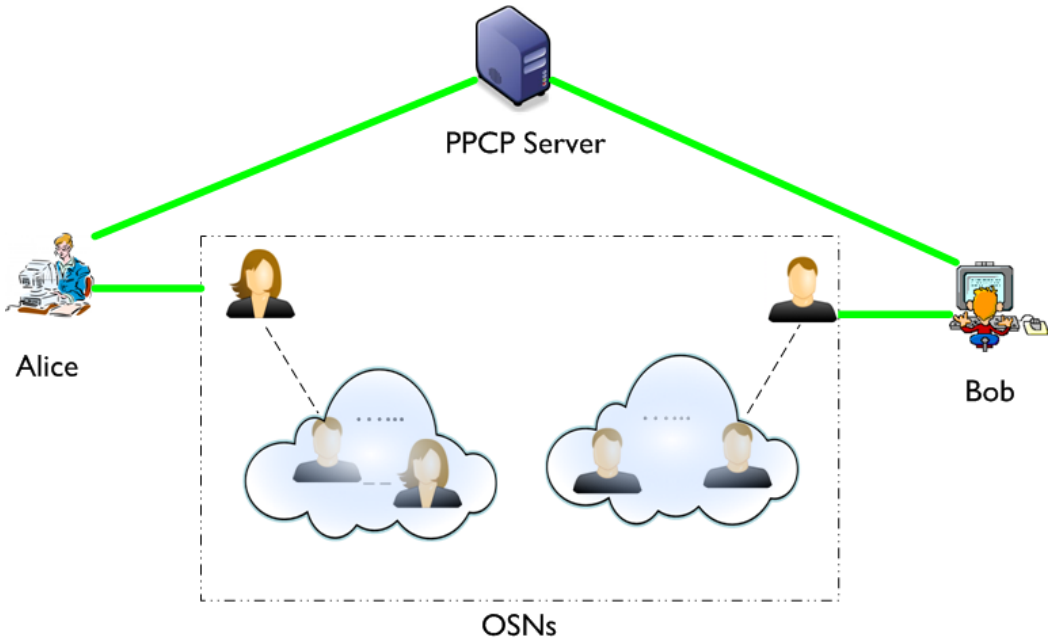
Profile Matching (Scenario 1)

- Leverage a number of concepts
  - Trust between friends
  - New data encryption algorithms
  - Secure two-party computation techniques
  - **Bob can be offline**



Profile Matching (Scenario II)

- Leverage a number of concepts
  - Heuristics of friendship structure
  - Secure two-party computation techniques
  - **Alice and Bob should be online at the same time**



Secure Channel Establishment

- A novel key establishment protocol, leveraging on
  - The PPCP server
  - The common private profile attributes between friends

Outline

- Issues with Social Networks
- Introduction to the PPCP Project
- Acknowledgement

Acknowledgement

- Financial support from NInet foundation
- Support from the STW program (through Kindred Spirits project)