EUROPEAN COMMISSION
DIRECTORATE-GENERAL
Joint Research Centre

Joint Research Centre

SWAMI Workshop afternoon session

Preparing for “dark” scenarios on AmI

Yves Punie & Ioannis Maghiros

ipts

Introduction

Work Package 2 objective

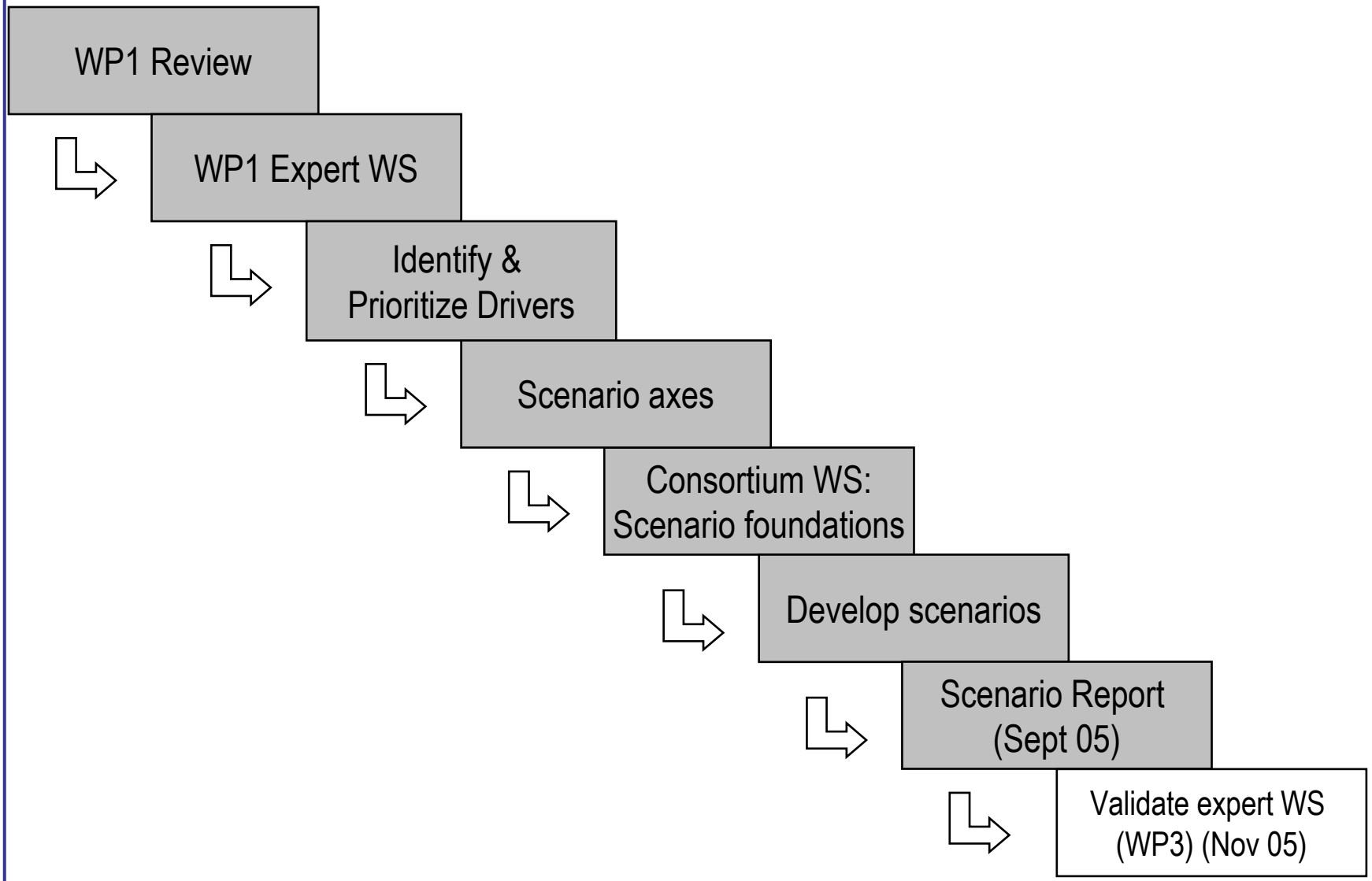
- Develop four dark scenarios on AmI
  - Highlighting the risks and vulnerabilities with regard to identity, privacy, security
  - Discuss the social, economic, legal, technological and ethical implications of these risks and vulnerabilities

Afternoon SWAMI Workshop objective

- Preparatory steps for developing the four scenarios:
  - Identify drivers and/or major issues that will orient the four scenarios and their positioning
  - Clustering and prioritisation of drivers and major issues
  - Leading to a preliminary positioning of four scenarios on two scenario axes

- NOT the objective to develop scenarios but a few words on the scenario exercise

Scenario building method



Dark scenarios

- To contrast the predominance of “bright” scenarios
- What can go wrong? What are the most important and most certain things that can go wrong?
- Alternative vision of the future we do NOT want to become reality
- But no doom scenarios either (everything goes wrong)
- Highlighting risks and vulnerabilities and discuss implications to better inform policymakers and developers
- Pro-active, rather than reactive: ensuring a ‘successful AmI’
- Citizen/user perspective (a day in the life of…)

E.g. if person recognition does not work and automatic door does not open:

INTENDED/
UNINTENDED

- Who is responsible/liable? (legal)
- What are the solutions? (technological and non-technological)
- Who will pay? (economic)
- How will users react? (social)

Afternoon sessions

Session 1 (1h30)

- Post-it session to identify drivers/issues on the risks and vulnerabilities of a future AmI world, with special attention to identity, privacy and security.
- Drivers are the forces that may shape the future in a certain direction (<-> trends are more certain: e.g. demographic evolution)
- Write the 2-3 most important ones on post-it
- Collect, discuss and organise them

Key Question: Driver for AmI but what can go wrong?

e.g. Profiling – my personal information gets stolen or my privacy invaded

e.g. DRM: not being able to make a private copy

e.g. Weblogs: can you delete history, archives?

Session 2 (1h15)

- Clustering in 5-10 groups
- Prioritize (high-low impact & high-low certainty)

AmI Drivers

Profiling
Impact 5 - Certainty 3

Cyber trust
Impact 4 - Certainty 3

DRM
Impact 5 - Certainty 2

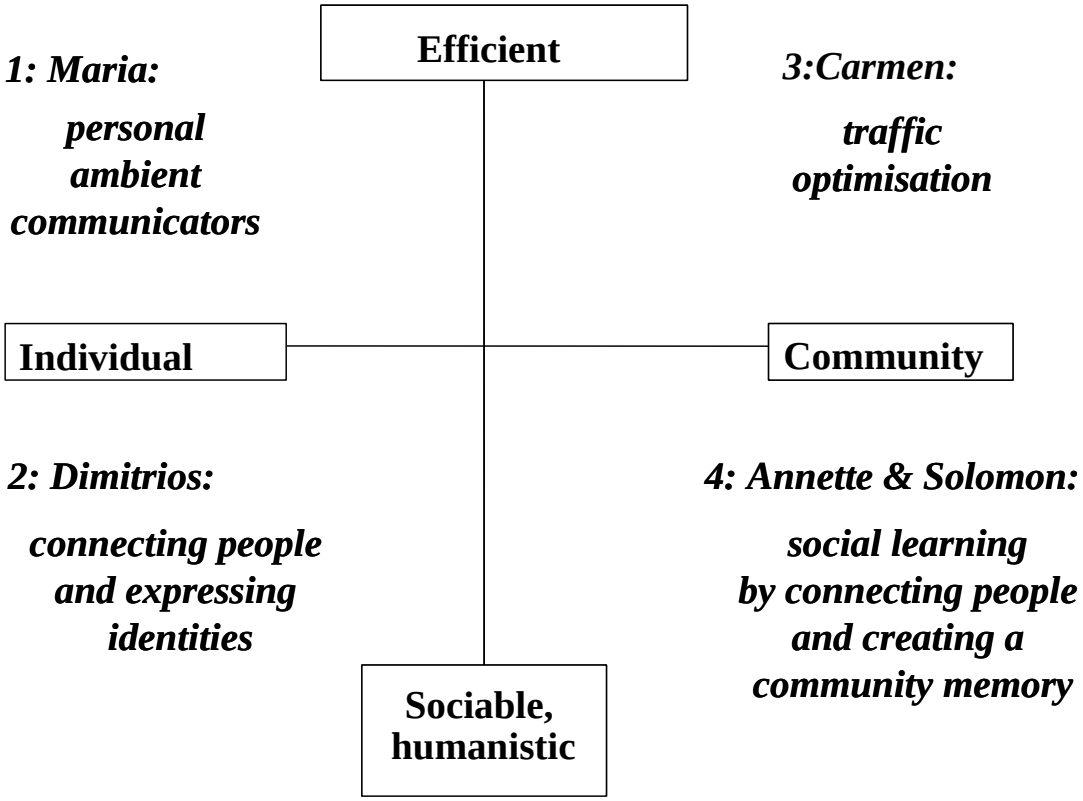
Digital Territory
Impact 4 – Certainty 2

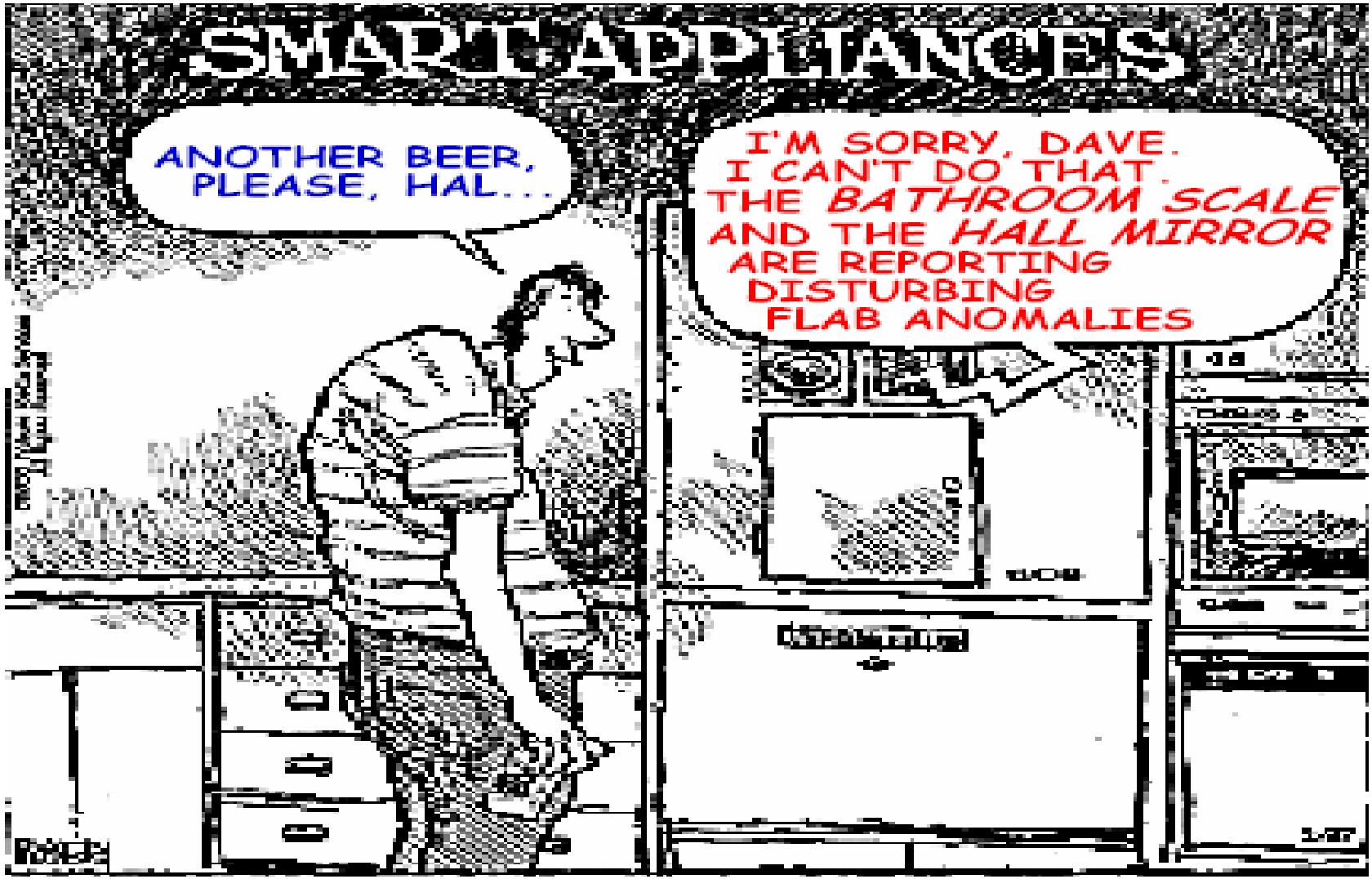
Technology **Social**

Economic **Legal**

Impact 5: High –> 1: Low

Certainty 5: High –> 1: Low





Cartoon by Jeff MacNelly

Definitions

A “risk” is the probability that a threat will act on a vulnerability to cause an impact

A “threat” is an unwanted (deliberate or accidental) event that may result in harm. Exploiting a vulnerability is a threat

A “vulnerability” is a weakness in the system