

Are households prepared for a connected future?

Relink open conference, OsloMet, June 11th 2019





RELINK PROJECT

- questions and ambitions

ARDIS STORM-MATHISEN,

RESEARCH PROFESSOR

CONSUMPTION RESEARCH NORWAY - SIFO

RELINK – Relinking the weak link

Building resilient digital households through interdisciplinary and multilevel exploration and intervention

Project funded by Research Council of Norway, IKTPluss, 2019- 2023



<https://blogg.hioa.no/relink>

Home Project Consortium News & Events Resources ▾ Contact

**RELINK - RESEARCH TO CONSTRUCT
KNOWLEDGE & RAISE AWARENESS
ABOUT DIGITAL VULNERABILITIES IN
CONNECTED HOMES**

Builds on previous RCN projects, i.e:

- Homerisk
- RFID in Society
- Contextualizing adolescents' egaming
- Gendering ICT

RELINK – Ambitions

Primary objectives

- To advance the state of the art in **knowledge** on security, IoT, and connected households.
- To map out technological and social infrastructures of consumer household IoT and the scope of digital vulnerabilities.
- To develop and deploy current and future scenarios of the risks and opportunities of technologies in connected households.
- To develop a toolkit for consumers security and strategies for dealing with risks related to everyday use of IoT.

- **Secondary objectives**
- To develop a deeper understanding and **awareness** among consumers of cybersecurity issues related to smart living.
- To promote citizen involvement and societal debate on security and consumer IoT.
- To inform policy on IoT, security, Big Data, and privacy.

Focus on households

- **Households, a core unit of society**
 - Socio-material framework that provides privacy, shelter, comfort, security and welfare for individuals
 - Hub for orchestrating decision-making, activities and roles across generations
- With the influx of internet, IoT and smart devices, **households:**
 - **are increasingly becoming sites for**
 - **Interventions** to address societal challenges (i.e. 'smart homes', e-health and welfare technologies)
 - **Market place** – consumer practices and decisions
 - Accessing and using a range of '**critical societal functions**'
 - **Digital vulnerabilities in society**
 - **left with large responsibilities**
 - Making safe choices in the digital market
 - Ensuring digital maintenance and performing security/privacy routines
 - Building competence required to handle digital risks



Digital risks and vulnerabilities

- Digital risks interact/are complex
- Complexity and incalculability will continue to increase
 - 'More smart' products & services (IoT) , new transactional regulations (PSD2)
- Technology paradoxes are difficult to navigate
- The everyday flows and logics in private life is of another kind than in formal institutions
- We need, but do not have
 - Sufficient knowledge about what the challenges are
 - Integrated initiatives to increase digital competence among consumers
 - Digital vulnerability risk-assesment tools and resources that can support households

**Are households prepared for a connected future?
– or a weak link?**



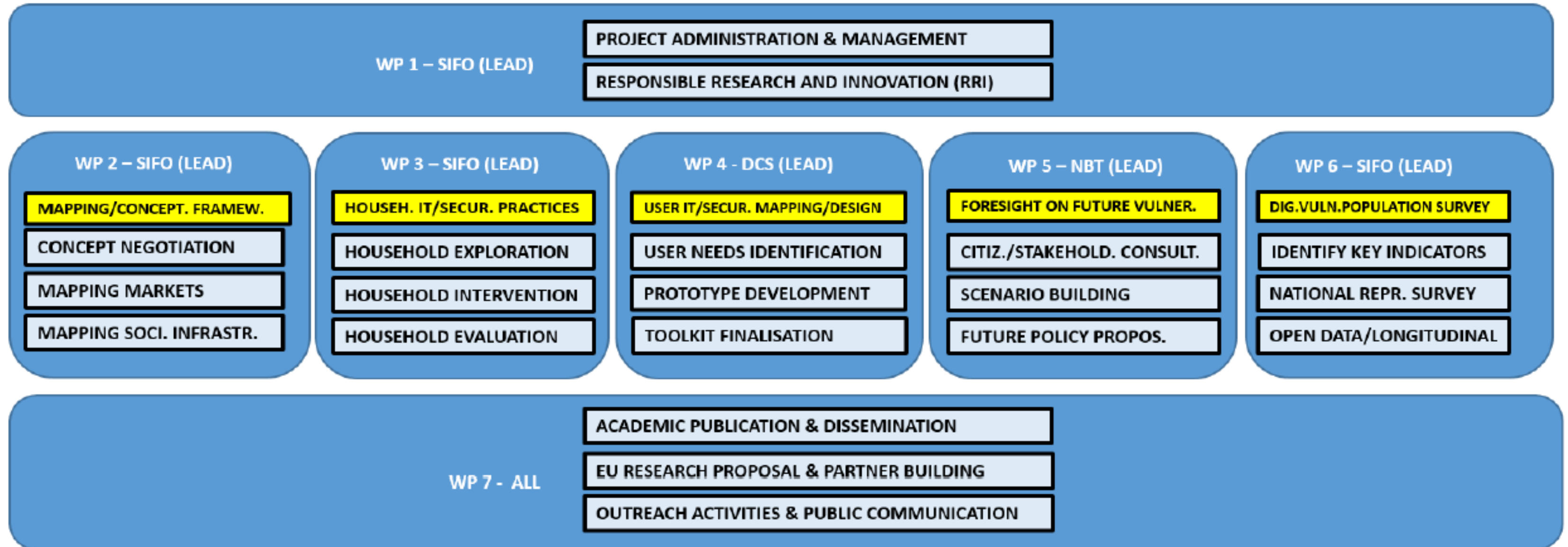
RELINK – Questions

Main RQ:

- *What roles do socio-technical practices and infrastructures play in shaping security risks in technologies of the home and*
- *What tools and interventions can be developed to enable digitally resilient households?*

- Approach:
 - Bottom-up, practice-oriented, socio-technical
- Key research site:
 - Diverse ‘connected homes’ (families with children, young couples, elders, functionally impaired) in Norway
- Means of knowledge construction:
 - Multi-methodological, cross-sectorial collaboration & participatory co-creation between Social science & IT/human-computer interaction researchers, IoTprojects & stakeholders/experts & households

Work packages



Work packages & methods

1. Administration & management
 - Financial, ethical, legal guidelines & RRI
2. **Mapping and developing framework for digital vulnerability analysis** of societal infrastructures in households (concepts, devices & networks, markets, policies)
 - *Desk-top document analysis & workshops*
3. **Exploration, intervention and evaluation of IT security infrastructures, practices and vulnerabilities in households.**
 - *Digital-visual-sensory ethnographic fieldwork & technical walkthroughs (mapping and testing vulnerability of digital practices/actor-networks inkl. devices, applications/interfaces and networks), interviews (consumer experiences, attitudes and strategies) & workshops*
4. **Building tools for everyday risk management and user awareness.**
 - *Computational techniques (testing vulnerability of data and developing future scenarios), co-design work-shops (visualizations, prototyping)*
5. **Foresight and development of future scenarios**
 - Scenario building, fore- and back casting, citizen panels, co-design workshops (visualizations, prototyping and personas)
6. **Digital vulnerability population survey**
 - Develop indicators for representative survey (comparing with other available surveys)
7. Communication, dissemination and future research impact agenda

RELINK partners

Norwegian partners

Consumption Research Norway (SIFO), Oslo Metropolitan University (OsloMet) Norway

Department of Computer Science (DCS), Oslo Metropolitan University (OsloMet) Norway

Teknologirådet/Norwegian Board of Technology (NBT) Norway

International partners

The Consumer Society Research Centre (CSRC), University of Helsinki Finland

The Department of Product and Systems Design Engineering (DPSDE), University of Aegean Greece

Rathenau Instituut (RI) Netherlands



Collaborative projects

Dept of Security and Crime Science, University College London (UCL), England

PETRAS IoT Research Hub

Center for Cyber and Information Security (CCIS), NTNU, Norway

H2020 - GHOST project

Advisory board

Dept. of Informatics (IFI), Univ. of Oslo, Norway

IT University of Copenhagen (ITU), Denmark

The Oslo School of Archit. & Design (AHO), Norway

Centre for Gender Research, Univ. of Oslo, Norway

George Mason University, (GMU), United States

European Commission, DG JUST, Belgium

Experts/stakeholders

Nkom

Forbrukerrådet

Standard Norge

DSB

NSM

Datatilsynet

Difi

NAV

Buudir

Skatteetaten

DNB

Nets

Safe4 Secur. Gr.

OSLOMET



OSLOMET



OSLO METROPOLITAN UNIVERSITY
STORBYUNIVERSITETET

Collaborative projects



PETRAS IoT Research Hub,
Department of Security and Crime Science,
University College of London

Experts and stakeholders



RELINK partners

Norwegian partners

Consumption Research Norway (SIFO), Oslo Metropolitan University (OsloMet) Norway

Department of Computer Science (DCS), Oslo Metropolitan University (OsloMet) Norway

Teknologirådet/Norwegian Board of Technology (NBT) Norway

International partners

The Consumer Society Research Centre (CSRC), University of Helsinki Finland

The Department of Product and Systems Design Engineering (DPSDE), University of Aegean Greece

Rathenau Instituut (RI) Netherlands

PHD

PHD

Collaborative projects

Dept of Security and Crime Science, University College London (UCL), England

PETRAS IoT Research Hub

Center for Cyber and Information Security (CCIS), NTNU, Norway

H2020 - GHOST project

Advisory board

Dept. of Informatics (IFI), Univ. of Oslo, Norway

IT University of Copenhagen (ITU), Denmark

The Oslo School of Archit. & Design (AHO), Norway

Centre for Gender Research, Univ. of Oslo, Norway

George Mason University, (GMU), United States

European Commission, DG JUST, Belgium

Experts/stakeholders

Nkom

Forbrukerrådet

Standard Norge

DSB

NSM

Datatilsynet

Difi

NAV

Buudir

Skatteetaten

DNB

Nets

Safe4 Secur. Gr.

Are households prepared for a connected future?



LOOKING FORWARD, LEARNING FROM THE PAST – POLICIES & PROSPECTS

0920-0940 **The European citizen-consumer – rethinking digital competence in the era of IoT?**

- Antonia Fokkema, DG Justice and Consumers, European Commission.

0940-1000 **Will IoT technology actually reshape our future – or is it just another hype?**

- Dhoya Snijders, Rathenau Institute

1000-1020 **The human weak link in national security systems**

- Roar Thon, The Norwegian National Security Authority (NSM)

1020-1040 Coffee break

CONNECTED PEOPLE, CONNECTED HOMES – CHALLENGES & EXPERIENCES

1040-1100 **The home as a data hub – security challenges and commercial pressures**

- Geir Birkheim, Safe4

1100-1120 **Safeguarding Home IoT environments – lessons from the H2020 GHOST project**

- Marios Anagnostopoulos, NTNU

1120-1140 **Cyber-hygiene at home – lessons from PETRAS IoT research projects**

- John Blythe, UCL/CybSafe

1140-1200 **IoT in Norwegian Homes – preliminary findings from Relink survey**

- Dag Slette-meås, SIFO/OsloMet

1200-1230 **Panel debate – presenters discuss challenges and opportunities**

- Moderator: Joakim Valevatn, Norwegian Board of Technology

1230-1400 Lunch for all conference participants

Are households prepared for a connected future?



LOOKING FORWARD, LEARNING FROM THE PAST – POLICIES & PROSPECTS

0925-0950 **The European citizen-consumer – rethinking digital competence in the era of IoT?**

- Antonia Fokkema, DG Justice and Consumers, European Commission.

0950-1015 **Will IoT technology actually reshape our future – or is it just another hype?**

- Dhoya Snijders, Rathenau Institute

The human weak link in national security systems

- Roar Thon, The Norwegian National Security Authority (NSM)

1015-1030 *Coffee break*

CONNECTED PEOPLE, CONNECTED HOMES – CHALLENGES & EXPERIENCES

The home as a data hub – security challenges and commercial pressures

- Geir Birkheim, Safe4

1030-1155 **Safeguarding Home IoT environments – lessons from the H2020 GHOST project**

- Marios Anagnostopoulos, NTNU

1155-1120 **Cyber-hygiene at home – lessons from PETRAS IoT research projects**

- John Blythe, UCL/CybSafe

1120-1155 **IoT in Norwegian Homes – preliminary findings from Relink survey**

- Dag Slettemeås, SIFO/OsloMet

1155-1230 **Panel debate – presenters discuss challenges and opportunities**

- Moderator: Joakim Valevatn, Norwegian Board of Technology

1230-1400 *Lunch for all conference participants*