# Authoring Digital Interactive Narratives

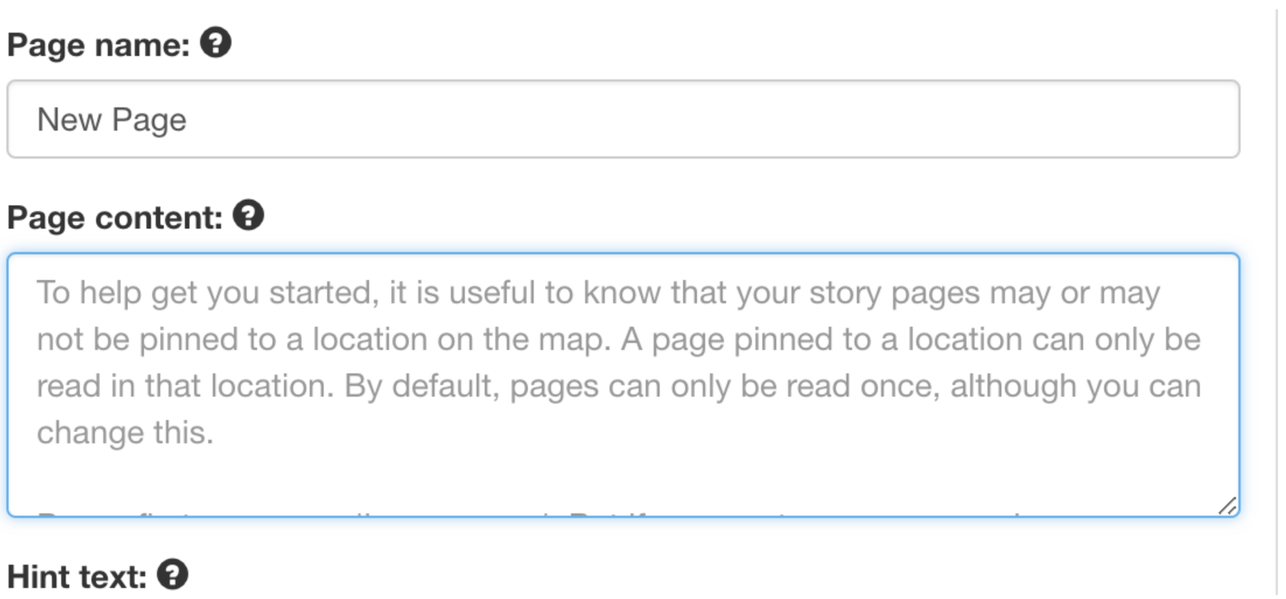
A study around the experience of **authoring** with **digital interactive authoring tools**

By **Sofia Kitromili** | S.Kitromili@soton.ac.uk | PhD Web Science | 2017-2020

Supervisory team: Dr. David Millard, Dr. James Jordan

**Centre for Doctoral Training in Web Science Innovation**


Writing in the 1940's required three things; ideas, paper and a writing instrument. A great transformation has risen with regards to the writing instruments made available for concerned authors, to expand and elaborate their ideas since the introduction of the world wide web. Pen made way for typewriters. Typewriters made way for word processors, and word processors made way for digital interactive writing tools. Tools that allow new, interactive and more complex forms of storytelling to be produced.


The project seeks to explore digital, modern forms of interactive storytelling and examine how new mediums impact the ways which we tell stories, and subsequently the stories we are trying to tell. The research will focus on the experience of writing interactive narratives by conducting a set of authoring experiments against a number of digital interactive authoring tools. To support the knowledge behind the authorial practise the project will look into questioning and interviewing authors in the relevant communities on their informed decisions to write a story with an interactive authoring tool, their decisions on how they plan to write a story and the procedures they follow. Research questions will be looking to answer how interactivity plays a role in the ways which authors choose to write a story, how they plan the story structure and what modifications they need to make when they encounter the writing tool.

With a similar account in mind the project may extend to the realms of cultural heritage and perform an authoring experiment that will remediate guided walking or otherwise navigational tours. This means that a potential authoring experiment will involve an interactive authoring tool that represents locative literature. In doing so, authors concerned will in fact be curators that will be questioned in the ways they organise, arrange and deliver stories of sites or artefacts. The knowledge will then be adapted into creating a digital locative experience. In doing so, research questions will extend to further answer how we currently plan and structure the ways we relay history through the mediums, what changes when interactivity is incorporated, what can a locative technology offer to unconnected spaces and what are the effects of remediating that which we already know as guided, walking or otherwise historical trailing tours.

UNIVERSITY OF Southampton

Digital Economy
Transforming Business and Society

# Feminist Twitter

## Why feminists use social media as political action

*Cat Morgan*

### Research questions

1. What is it about Twitter that facilitates feminists use of it for political reasons?
2. Is there a sense of solidarity amongst feminists on Twitter?
3. Why do feminists continue to use Twitter after being trolled?
4. Why do feminists use personal narratives as political action?

### Background

There is a trivialisation of gendered politics and feminism in patriarchal society that does not report on important issues. The Web is a transformative space that, along with the use of mobile technologies, provides alternative avenues for political action. Feminists are using Twitter increasingly to have their voices heard.

### Sociology of Twitter

- Unique politicised digital community
- Users create their own social networks which can act as an echo chamber
- By removing barriers of distance and geography Twitter is facilitating political discussion
- Power in the hashtag and the ability to disseminate information to a wide audience

### Research Design

- Semi-structured interviews – politicians, academics and activists
- Feminist Digital Ethnography – study of Feminist Twitter as an online community
- Case Study – Women's' Equality Party Conference 2018
- Personal reflections: in a community that I am studying and my own experience of trolling

### Online political action

- Blogging/Shared narratives – Everyday Sexism provides a perspective that is not present in patriarchal narrative and the media (Crossley, 2015)
- Mobilisation – organising offline action  such as meetings and marches (Carty, 2015)
- Campaigning – an online action that can have an offline action
- Slacktivism – showing support for a cause performed as like/favourite and disseminating as a share/retweet
- Clicktivism – Change.org and 38 Degrees: opinion sampling from a cross-section of society

References:
Carty, V., 2015. Social Movements and New Technology. Westview Press
Crossley, A.D., 2015. Facebook feminism: social media, blogs, and new technologies of contemporary US feminism. Mobilization 20, pp253–268

Images: B0red_vectors and Twitter logo

*Supervisors – Dr Matt Ryan, Dr Valentina Cardo & Dr Su White*

UNIVERSITY OF Southampton

# Smart, data-driven cities:

# Private harm for public good?

Jacqui Ayling

UNIVERSITY OF Southampton

RQ1: How does data flow in smart city applications?

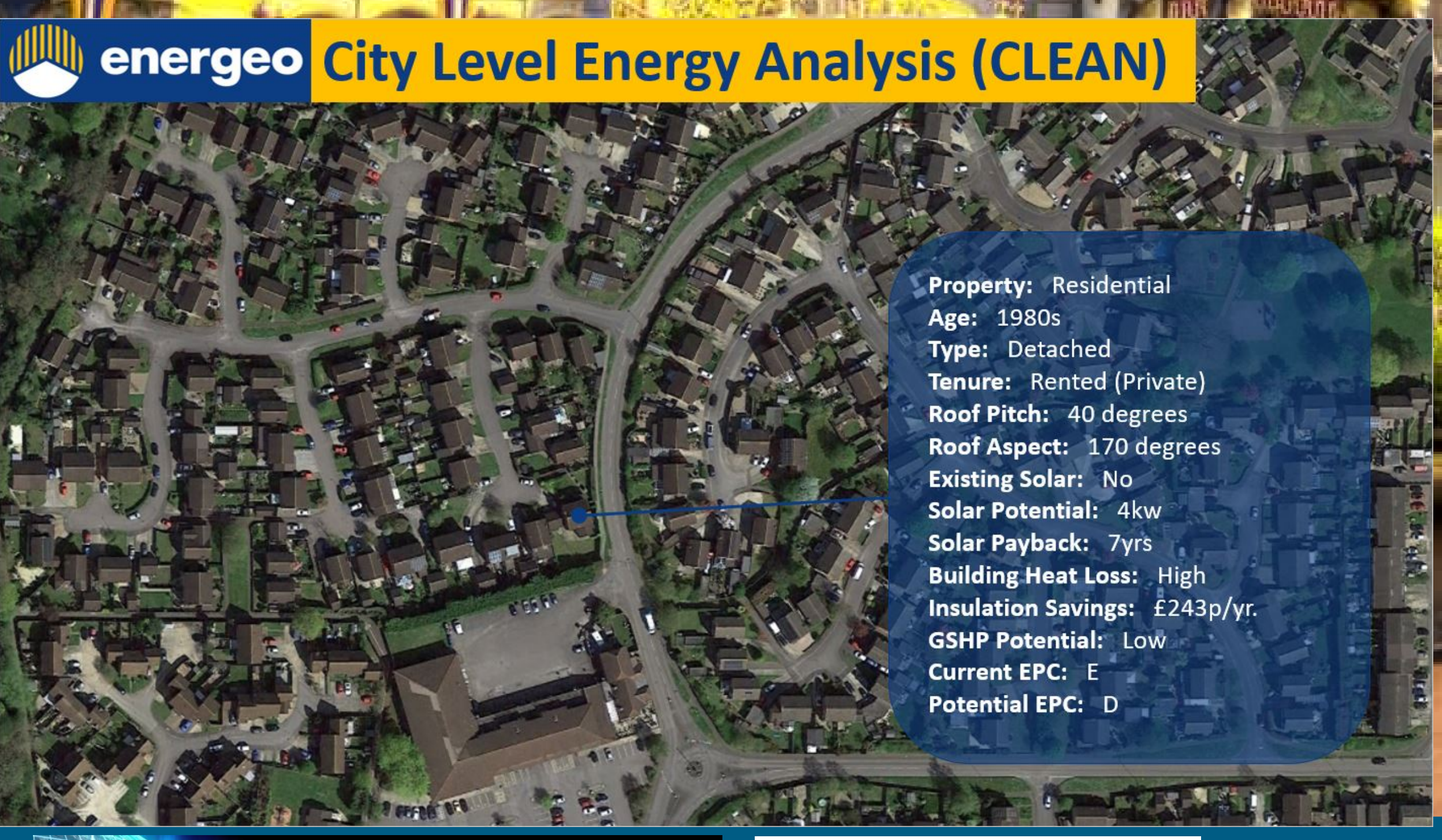
RQ2: What are the possible risks/harms from these data flows to individuals?

RQ3: Is it possible to mitigate any risks?

| Domain | Technology applications |
|---|---|
| Governance | E-government systems; online transactions; city operating systems; performance management systems; urban dashboards; citizen participation platforms; open data; hackathons |
| Security and emergency services | Centralised control rooms; digital surveillance; predictive policing; coordinated emergency response (flood, earthquake, hurricane, epidemics, civil unrest); CCTV |
| Transport | Intelligent transport systems; integrated ticketing; smart travel cards; bikeshare; real-time passenger information; smart parking; logistics management; transport apps; GIS; LIDAR |
| Energy | Smart grids; smart meters; energy usage apps; smart lighting; GIS; LIDAR; thermal imaging |
| Waste | Compactor bins and dynamic routing/collection |
| Environment | Sensor networks (e.g., pollution, noise, weather; land movement; flood management) |
| Buildings | Building management systems; sensor networks |
| Homes | Smart meters; app controlled smart appliances |
| Economy | Digital infrastructure; innovation hubs; open data; data markets |
| Health and wellbeing | E-health applications; resource allocation; public health; disease and epidemics; social services; home care |

| Domain | Categories of privacy breach | |
|---|---|---|
| Information collection | | |
| | Surveillance | Watching, listening to, or recording of an individual's activities |
| | Interrogation | Various forms of questioning or probing for information |
| Information processing | | |
| | Aggregation | The combination of various pieces of data about a person |
| | Identification | Linking information to particular individuals |
| | Insecurity | Carelessness in protecting stored information from leaks and improper access |
| | Secondary use | Use of information collected for one purpose for a different purpose without the data subject's consent |
| | Exclusion | Failure to allow the data subject to know about the data that others have about her and participate in its handling and use, including being barred from being able to access and correct errors in that data |
| Information dissemination | | |
| | Breach of confidentiality | Breaking a promise to keep a person's information confidential |
| | Disclosure | Revelation of information about a person that impacts the way others judge her character |
| | Exposure | Revealing another's nudity, grief, or bodily functions |
| | Increased accessibility | Amplifying the accessibility of information |
| | Blackmail | Threat to disclose personal information |
| | Appropriation | The use of the data subject's identity to serve the aims and interests of another |
| | Distortion | Dissemination of false or misleading information about individuals |
| Invasion | | |
| | Intrusion | Invasive acts that disturb one's tranquillity or solitude |
| | Decisional interference | Incursion into the data subject's decisions regarding her private affairs |

energeo City Level Energy Analysis (CLEAN)




## Use Case 1: Geospatial data for energy transformation systems

Is detailed geospatial data about my home personal data? What risks might be created by these insights?

UNIVERSITY OF Southampton
Web Science

EPSRC
Engineering and Physical Sciences Research Council

Jacqui Ayling
Email: J.A.Ayling@soton.ac.uk

University of Southampton Web Science Institute

Research Councils UK Digital Economy — Transforming Business and Society

EPSRC Pioneering research and skills

# History of Innovation in Web Technology: Evidence From US Patents

Maria Priestley[1] ✉, Thanassis Tiropanis[1], Tim Sluckin[2]

[1]Department of Electronics & Computer Science, [2]Department of Mathematics, University of Southampton

✉ mp5g15@soton.ac.uk

## Background

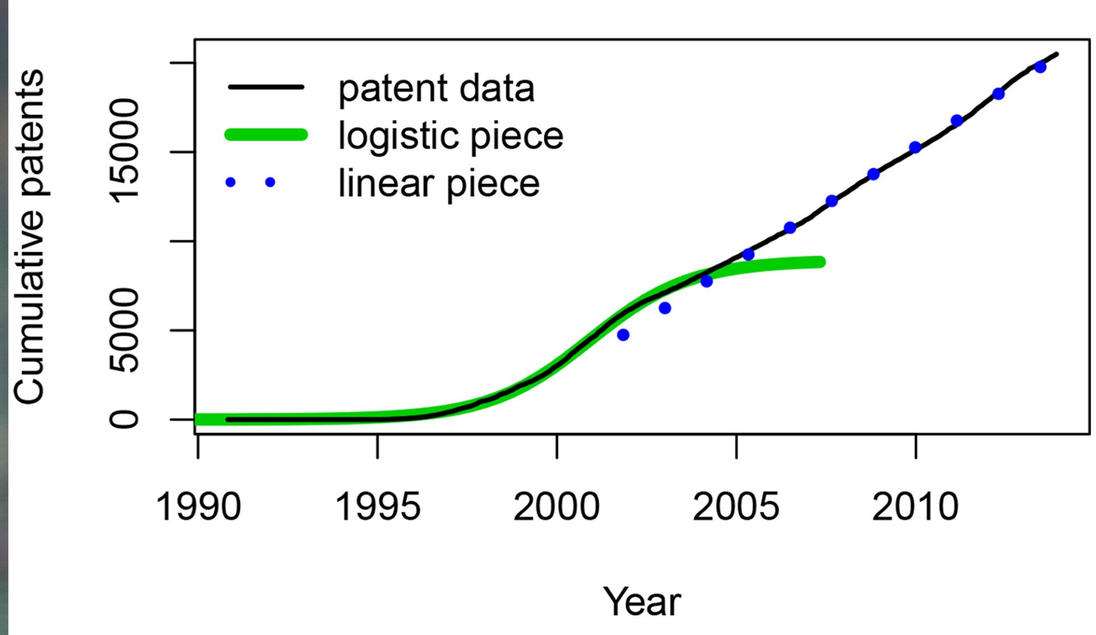
What we know about the development of Web technology has so far been based largely on anecdotal accounts and expert opinions. Compelling questions include whether the Web has grown exponentially, the timing of shifts (e.g. to Web 2.0), and the connection between Web development and major socio-economic events like the dot-com crash.

Our research aims to contribute quantitative evidence to such discussions.

## Dataset

We gathered 20,493 patented inventions related to the Web from the US patent record. Patents were selected using keywords based on technical infrastructures, data formats and protocols commonly used on the Web. The dataset spanned years 1990 to 2013.

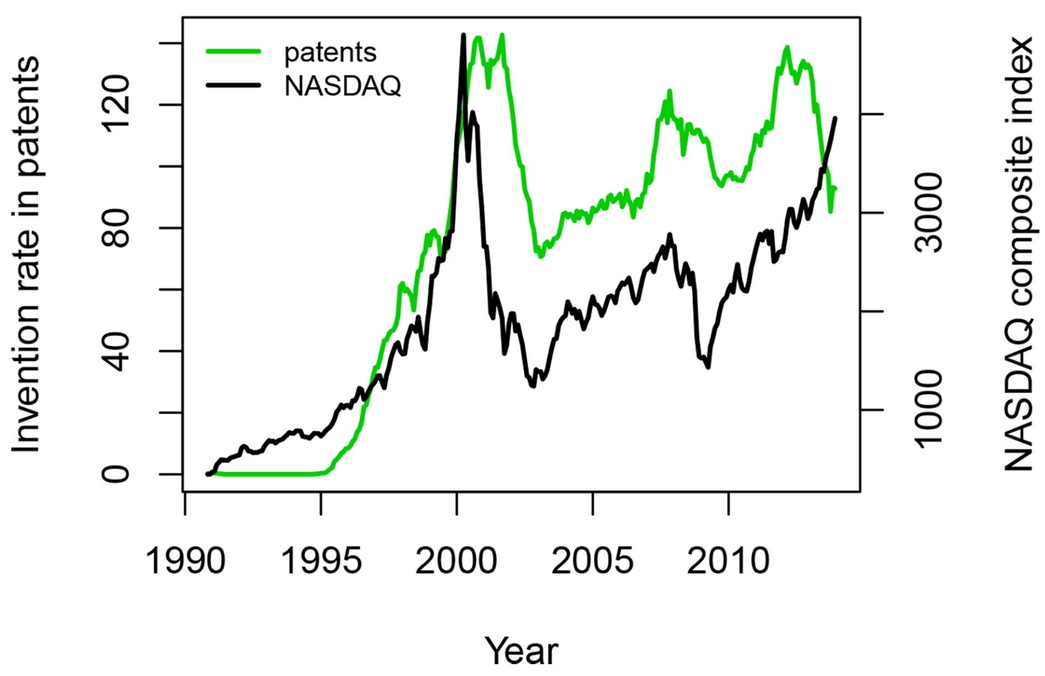
## Growth curve of Web tech patents




Inflection of patenting activity in year 2000 coincides with the timing of the dot-com crash.

Shift from logistic to linear growth since 2004.

## Stock market correlation




A statistically significant positive correlation between patenting rates in Web technology and the NASDAQ index ($r_p$ =0.17, n = 269, p < .05).

Patenting activity lagged behind the NASDAQ by approximately 6 months.

In other words, prior movements in the stock index could explain 17% of the variation in patenting activity occurring approximately 6 months later.

# How do populists' supporters engage online?

UNIVERSITY OF Southampton
*Centre for Doctoral Training in Web Science Innovation*

Justyna Jonak, Web Science, University of Southampon, Justyna.Jonak@soton.ac.uk.
Supervisors: Prof. Will Jennings, Associate Prof. David Millard.

UK Research and Innovation
Digital Economy
Transforming Business and Society

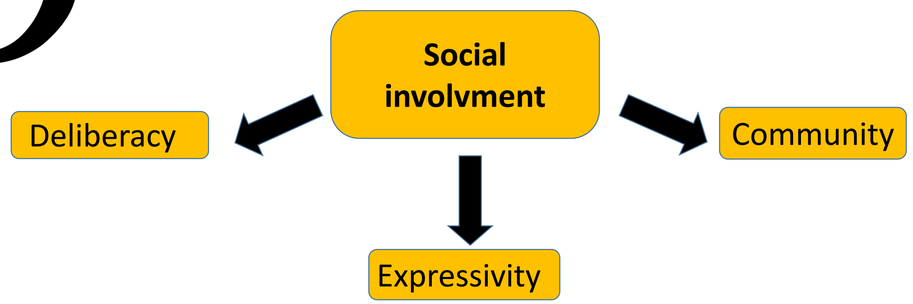
## 1 Background

- Populism is on the rise across the globe. The research in area of populism and social media has only recently gained its momentum.
- Populism on social media has been mainly considered from a supply-side perspective (politicians or political actors).
- Social media are also greatly used by people supporting populist's parties.
- There are almost non-existing studies considering a demand side of populism on the Web.

## 2 What does it mean to be politically active in an online environment? Different forms of political engagement

Social involvment ↔ Civic engagement ↔ Political participation

## 3 Social involvement and combing political science and communication studies




Social involvement though the lenses of communicative practices and different modes of democratic communication

## 4 Reaserch Aims and Questions

The aims

- to understand the political engagement of populists` supporters through the lenses of their communicative practices.
- to locate communication practices in a wider political landscape
- to develop a framework for studying an online political behaviour which takes into account the Internet's communication and information capabilities

The research questions

1. How do populist` supporters communicate online? What type of democratic communications do populist` supporters present on Facebook? Is there any dominant mode of democratic communication?
2. How users' behaviour on specific platforms and technological features are influencing certain modes of democratic communication?
3. Is there any difference in a democratic communication type between two groups that support the same populist party/movement on the same online discussion space?
4. Is there any difference in a democratic communication model presented by Kukiz`15 supporters between Facebook and Twitter platform?

## 5 Methodology and pilot study

- Mixed methods: qualitative content analysis, quantitative content analysis, comparative analysis

Pilot study:

- The initial pilot study concerned Facebook Fan Pages of people supporting Kukiz`15 – Polish populist's movement
- Two Facebook Fan Pages were selected: one formal and one informal
- Both groups showed different modes of democratic mode of communication despite of the fact that the analysis considered the same online space

References:
Ekman, J., & Amnå, E. (2012) Political participation and civic engagement: Towards a new typology. *Human Affairs*, Vol. 22,pp. 283–300. https://doi.org/10.2478/s13374-012-0024-1
Freelon, D. (2015) Discourse architecture, ideology, and democratic norms in online political discussion, *New Media and Society*, Vol. 17(5), pp. 772–791. doi: 10.1177/1461444813513259
Engesser, S., Fawzi, N. and Larsson, A. O. (2017) Populist online communication: introduction to the special issue, *Information, Communication & Society*. Taylor & Francis. Vol. 20(9), pp. 1–14. doi: 10.1080/1369118X.2017.1328525.

Supported by:

UK Research and Innovation

Digital Economy – Transforming Business and Society

University of Southampton

# PBX Toll Fraud – The Hidden Threat of NGN Telecoms

**Nathaniel McInnes** | Supervisors: Gary Wills, Ingi Lusmen, Ed Zaluska

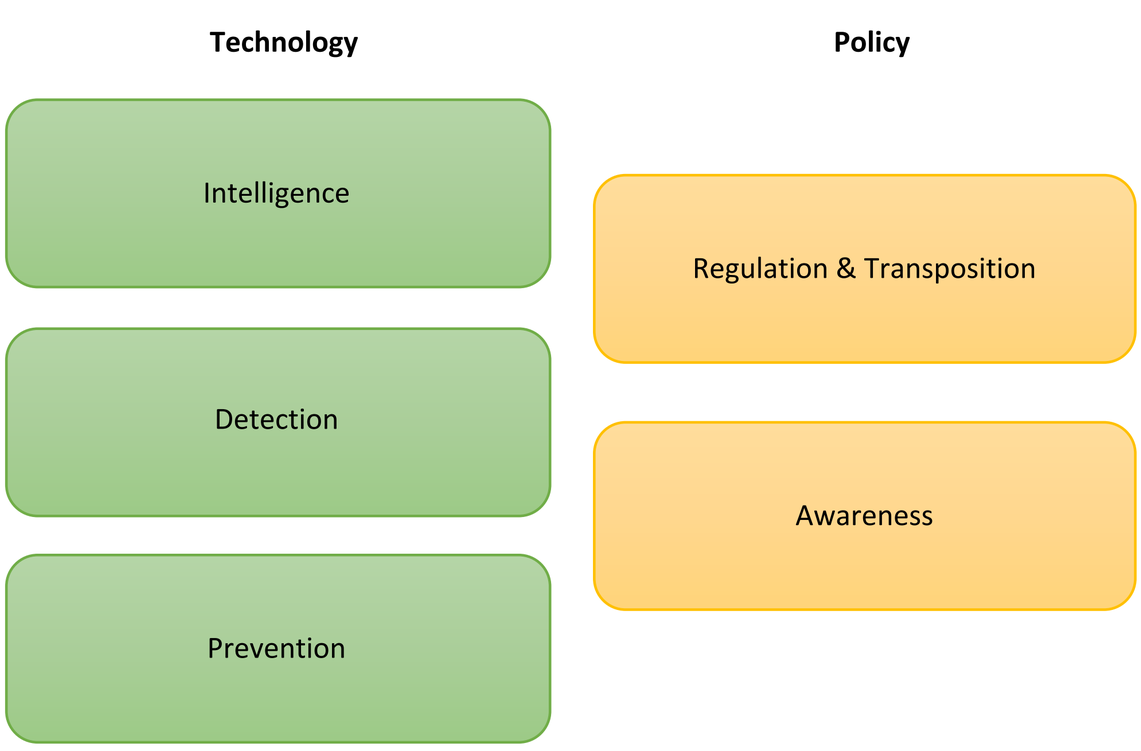
## 1. Background

Over the **past 10 years**, the way **businesses** run there **phone systems** (Private Branch Exchanges – PBXs) has **evolved into internet connected systems** (using Next Generation Networking - NGN Technologies such as VoIP) which **are designed for unified communications**. Thanks to the increase in their **web centric design** and **usability**, these phone systems **allow non-telephony professionals** to **build** their own **unified communication systems** with ease. With such ease and web centric design, advance **sophisticated attacks** are occurring which **results in billions of dollars a year being stolen from business** to **fund criminal** and **terrorism** related **activities**. This fraud makes use of **vulnerabilities** in the Global Telecom market **through policy holes** which **makes** it **almost impossible** to **trace** and claim funds back. **Individual attacks** can easily **cost** a business **tens of thousands of pounds per day**. **Previous** significant **research** is over **5 years old** and showed an **increasing problem** and **changing attack vector**. Current **legal instruments provide little assistance to businesses over this kind of fraud** and with NGN to become the new norm, it's paramount this fraud is mitigated.

## 2. Framework

Initial research has yielded significant directions of research. To assist in focusing the research, Research Questions have been created through a careful framework design which has been split into Technical and Policy Categories.

**VoIP Fraud Misuse Framework**




## 3. Initial Findings

To date a thorough background literature and a 3 month honeypot experiment have been conducted. The background literature has demonstrated a **policy landscape** where **there is confusion** of who is responsible and where **technical solutions** have only been theorized with **limited testing**.

The honeypot is a locked down PBX based on FreePBX (a popular Open Source PBX) with no connection to real VoIP Lines so no real calls could be generated.

The honeypot has demonstrated initial results of a problem that is significantly more problematic where **attacks** are upto **30 times larger** in scale than previous research and initial findings suggest **attackers attempt** to **hack** not only VoIP surfaces, but also **web surfaces** meaning **current solutions** could be **rendered useless**.

The **honeypot** has also **demonstrated** that **attackers are** a **botnet of infected PBXs** from well known manufactures suggesting once a PBX has been compromised, it forms part of the botnet itself.

**Most** forms of **attacks** resulted in **SIP Registration** attackers which attempt **to brute force username and passwords** in an attempt to gain access, although many attackers make direct call attempts to the PBX by attempting to **trick** the **PBX** into **believing** the **calls** were **made internally** and therefore not need authentication.

## 4. Future Work

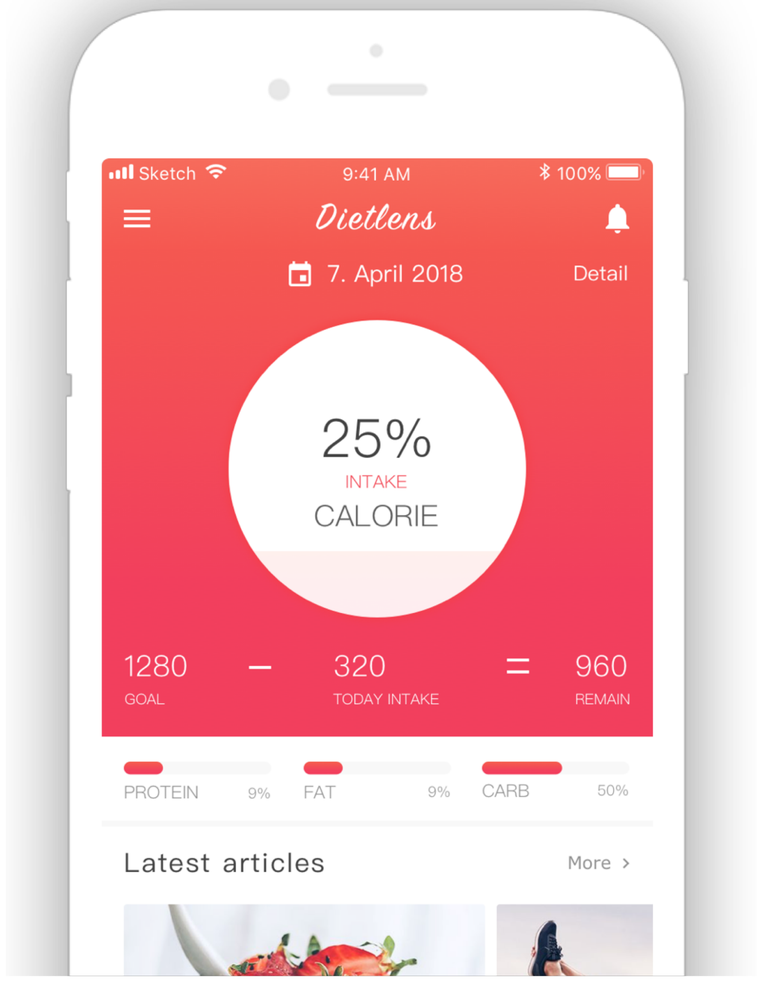
Future work is to further analyse the results of the honeypot to develop additional knowledge regarding an attack which can be used to develop a filter that can detect and prevent these kinds of attacks, but also gain primary knowledge through interviews with Policy stakeholders about legal provisions that can be used to mitigate some of the confusion around where responsibility lies.

# Investigating User Perception of Food Image Recognition in Dietary Tracking Applications


Jonathan Staniforth
js30g13@soton.ac.uk

Dr. Ming Zhaoyan
dcsming@nus.edu.sg

Prof. Dame Wendy Hall
wh@ecs.soton.ac.uk


DietLens app home page (Ming et al., 2018).

Nutrition applications educate people on the food they consume. However, users stop using such apps prematurely before they can gain health benefits, mainly due to the slow speed of entering information into the apps (Kerbs and Duncan, 2015).

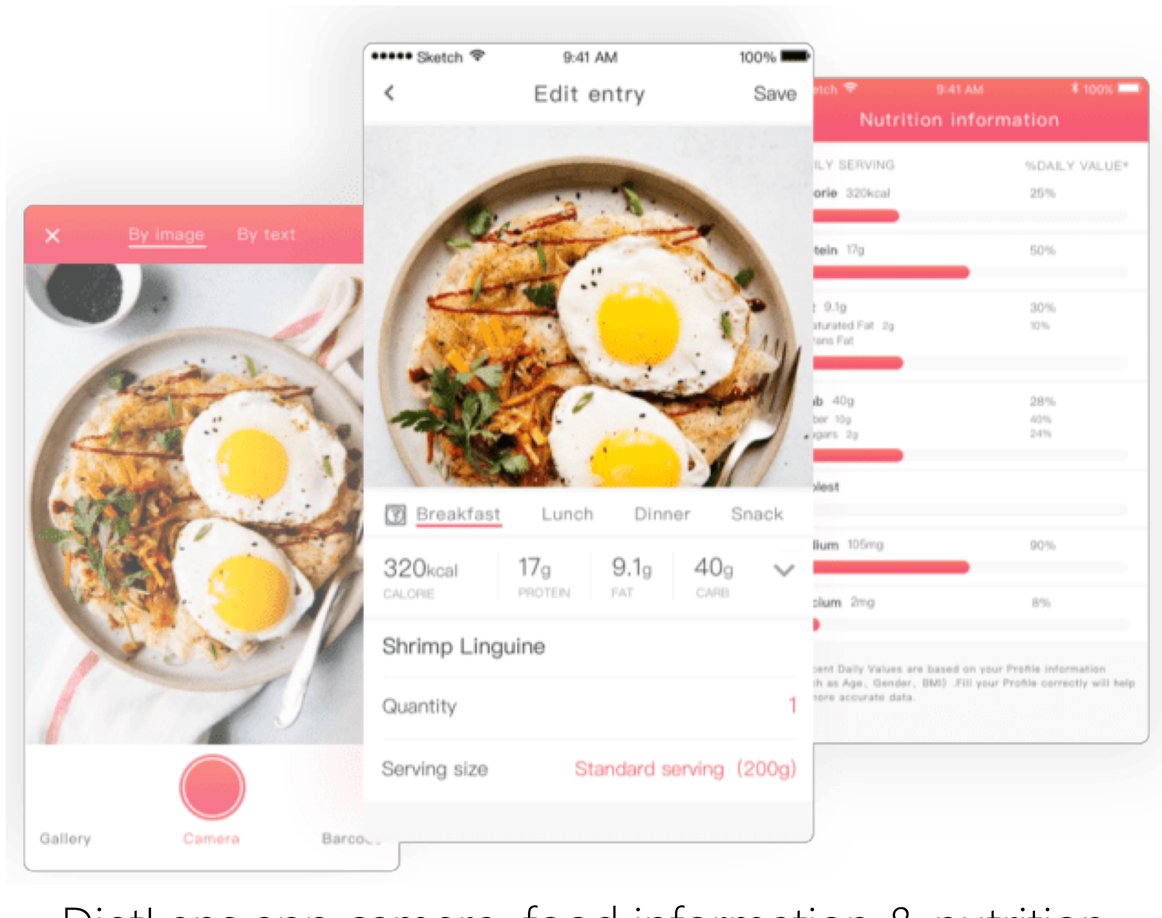
Image recognition technology promises to overcome this problem by quickly identifying food in a photo, instead of the user having to perform a text-based search. An example of such an application using this technology is DietLens (Ming et al., 2018), a dietary tracking app.

Additionally, DietLens utilises interactive machine learning to improve the system by accepting user feedback on its predictions (Kulesza, Burnett, et al., 2015; Stumpf et al., 2007). However, errors can occur through incorrect user feedback and require knowledge of users' perception to handle.

We will conduct a user study, taking a mixed methods approach (Creswell and Clark, 2006), and examine the DietLens app, focusing on:

- affordances of food image recognition as a data entry method;
- user motivation;
- user interactions;
- and, user engagement over time.

We will also perform a clinical study to understand how medical professionals view the app. The findings will help to improve the implementation of such technology from a user perspective and in a health app context.




DietLens app camera, food information & nutrition information pages (Ming et al., 2018).

## References


Creswell, J. W. and Clark, V. L. P. (2006) Designing and Conducting Mixed Methods Research. 1st edn. Sage Publications, Inc.

Krebs, P. and Duncan, D. T. (2015) 'Health App Use Among US Mobile Phone Owners: A National Survey', JMIR mHealth and uHealth, 3(4), p. 101.

Kulesza, T. et al. (2015) 'Principles of Explanatory Debugging to Personalize Interactive Machine Learning', in Proceedings of the 20th International Conference on Intelligent User Interfaces - IUI '15. New York, New York, USA: ACM Press, pp. 126–137.

Ming, Z. et al. (2018) 'Food Photo Recognition for Dietary Tracking: System and Experiment', in 24th International Conference on Multi Media Modelling (MMM). Bangkok, Thailand.

Stumpf, S. et al. (2007) Interacting Meaningfully with Machine Learning Systems.



A Joint Research Collaboration between

NUS National University of Singapore · Tsinghua University · University of Southampton

Our research is supported by the National Research Foundation, Prime Minister's Office, Singapore under its IRC@SG Funding Initiative.

# Privacy Challenges in the Smart Home

Robert H. Thorburn
R.H.Thorburn@soton.ac.uk

UNIVERSITY OF Southampton

## 1.Background

The Internet of Things (IoT) is steadily marching towards its headline goal of delivering cheap ubiquitous computing into every facet of society, from the workplace to the home.

As one of the most prominent areas of use for IoT devices, Smart Home applications stand out not just for their potential benefits and rapid adoption, but also for their extensive catalogue of failures.

This investigation aims to analyse data flows generated by Smart Home devices, comparing these findings to regulatory requirements and core data protection principles.

## 2.The Testbed

The testbed contains a selection of commercial smart home devices, including a core set from one supplier.

All devices connect to a smartphone and/or a Raspberry Pi, where the Pi hosts the closed network with no other devices present. TCPdump was used on the Raspberry Pi to capture network traffic, which was then analysed on a PC using Wireshark.

Two central questions answered by using the testbed were:

- What are typical data flows in a Smart Home?
- What are the main privacy, data protection and regulatory failures associated with data flows in the Smart Home?

## 3.Results

**Privacy risks due the lack of consent:**

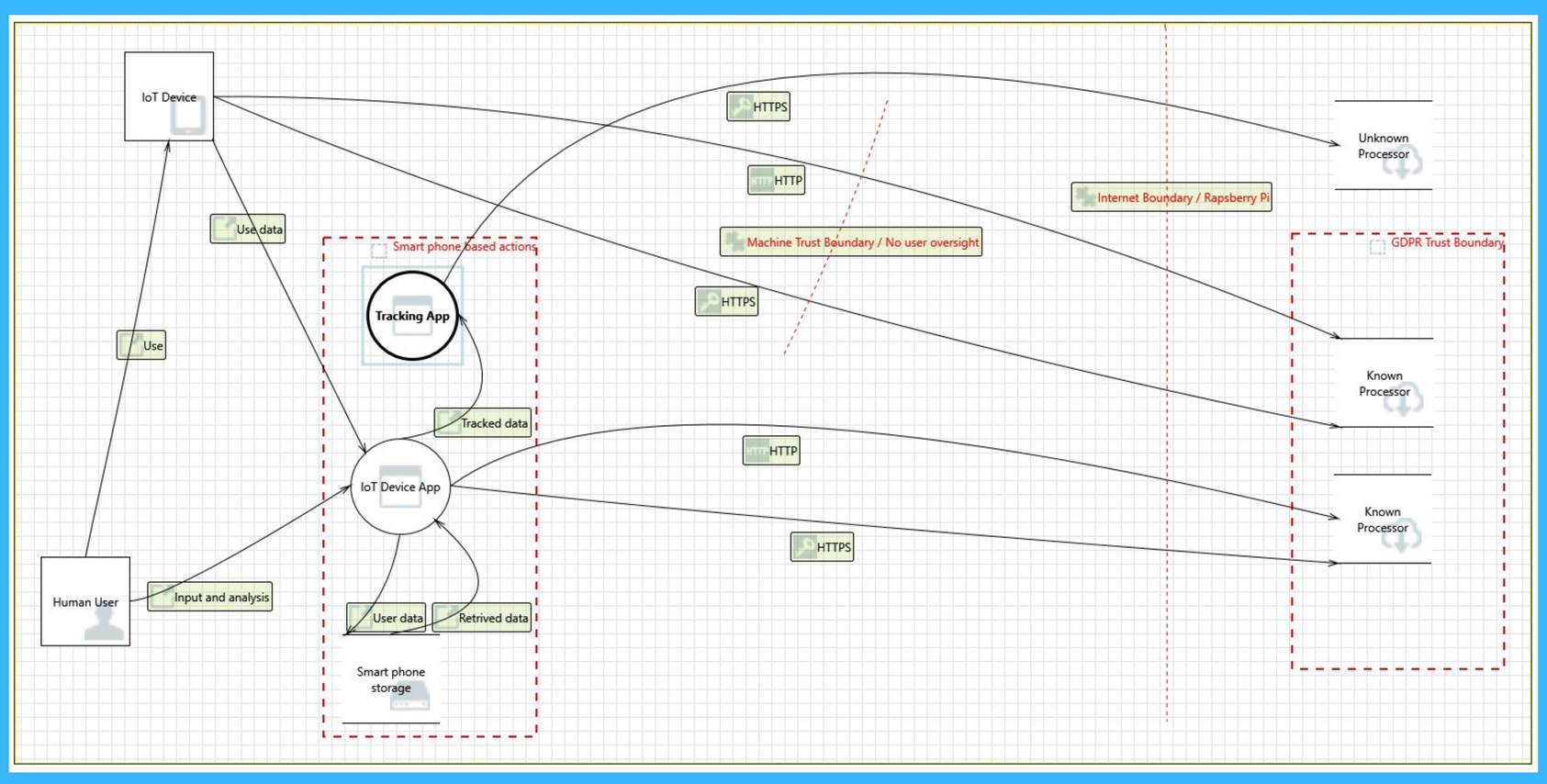
- The controller is not able to demonstrate that the data subject provided their consent.
- Consent is not gained in relation to documentation which is easily accessible and intelligible.
- Data subjects are unable to withdraw their consent since it was not correctly obtained in the first instance.
- Risk: personally identifiable data is collected and processed without a binding agreement between data subject and controller thereby undermining the data subject's legal protection.

**Privacy risks in the form of a purpose limitation breach:**

- Data collected beyond stated purposes.
- The controller does not explicitly declare data collection, nor is the collected data specified.
- Risk: processing and potential profiling exceeds that which the data subject has agreed to. Any potential breach or leak could have a greater impact on the data subject, while their ability to mitigate the negative impact will be reduced.

**Data protection principles breached:**

- Data minimisation, since more data is collected than needed to provide the agreed upon service.
- Availability and Intervenability, since there is no way for data subjects to interact with the data collected.
- Transparency, due to the trackers and their functioning not being presented to the data subject.
- Data confidentiality is breached through the use of hidden third-party processors with no formal link to the data subject.
- Transparency failures due to lacking documentation, opaque data processing processes lacking application of GDPR principles at every level of data processing.
- Intervenability is also brought in to question since the ability of data subjects to exercise their rights against third-party processors remains unclear.




**Worst Performers**

- One or more tracking apps
- Missing or hidden policies
- Circumvents user control

**Best Performers**

- No or limited tracking
- Clear policies
- Full transparency

UNIVERSITY OF Southampton Web Science

EPSRC Pioneering research and skills

Supervisors: Dr Federica Paci, Professor Sophie Stalla-Bourdillon and Dr Federico Lombardi

GCHQ

Cybersecurity Southampton