Privacy Therapy with Aretha: What If Your Firewall Could Talk?

William Seymour, University of Oxford | william.seymour@cs.ox.ac.uk

Introduction

Maintaining privacy and security in the networked home is wicked problem. At the same time, voice assistants (VAs) such as the Amazon Alexa and Google Assistant have quickly risen in popularity, becoming the centre of the smart home.

This presents an opportunity: what if firewalls and voice assistants were combined? The conversational nature of today's top assistants could allow for something that's missing from the modern smart home: *conversations* about privacy and security.

Continuing previous research on the concept of 'respectful' smart home devices, this work presents the Aretha project: a prototype voice assistant that allows users to have privacy and security conversations with their firewall.

Background

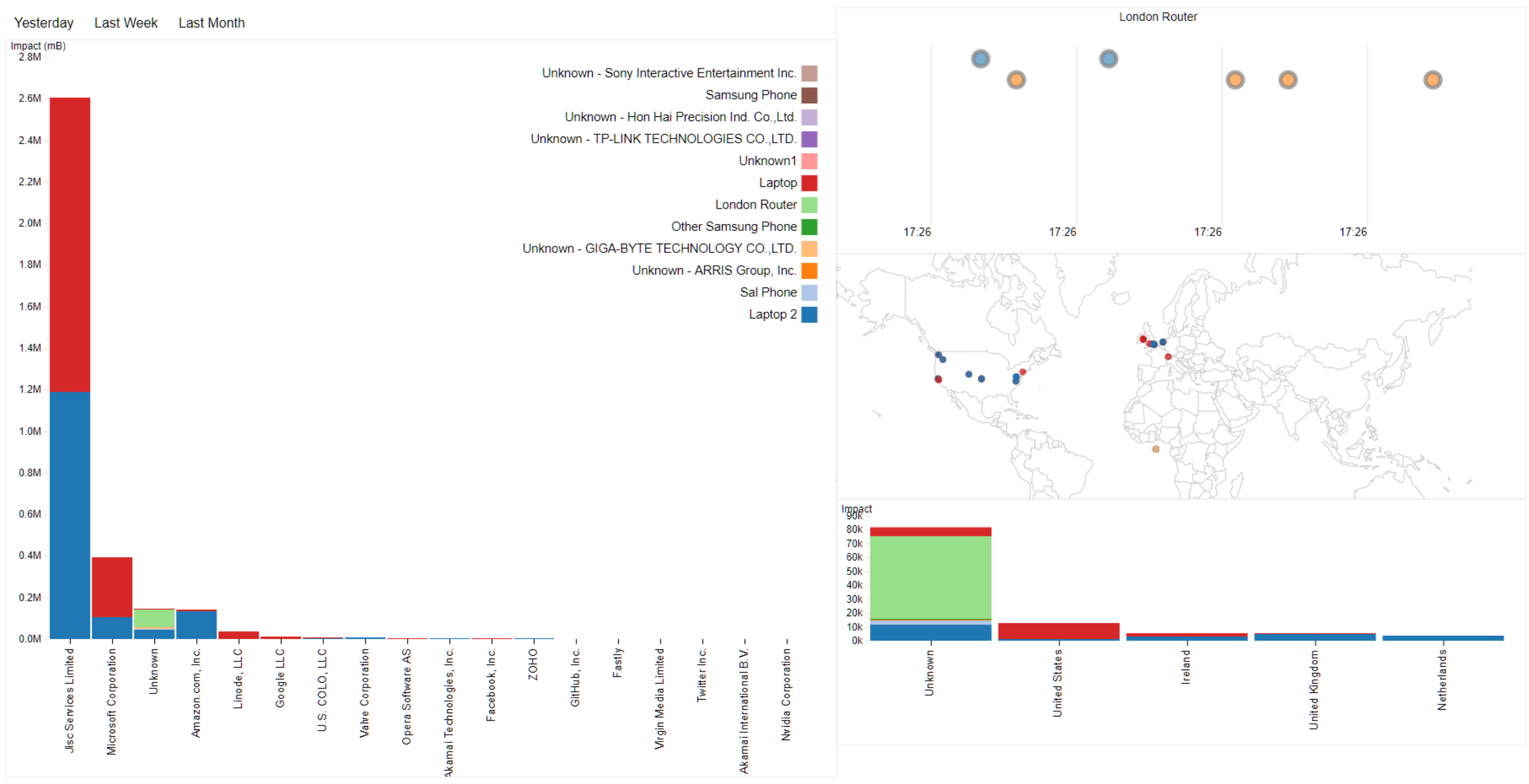
Voice Interfaces
Pioneering work by Reaves and Nass showed that voice interfaces can often trigger similar responses in humans to interpersonal communication [2]. For example, interactions with VAs are often positive even when failing to fulfil their functional objectives [3], and social responses to computers are automatic and unconscious [2].

Placed at the centre of the smart home, VAs are observe users across privacy boundaries, often leading to violations of privacy contexts.

Smart Home Security & Privacy
Previous studies exploring user understanding of smart phones [4] and smart homes [5] show a poor level of understanding about where personal data is sent.

This is often conceptualised as poor situational awareness, but it is unlikely that the users of any skill level could interpret the volume of information required, leading Van Kleek to conclude that the most effective tools in this space are likely to be those that support user decision making with analysis and automation [3].

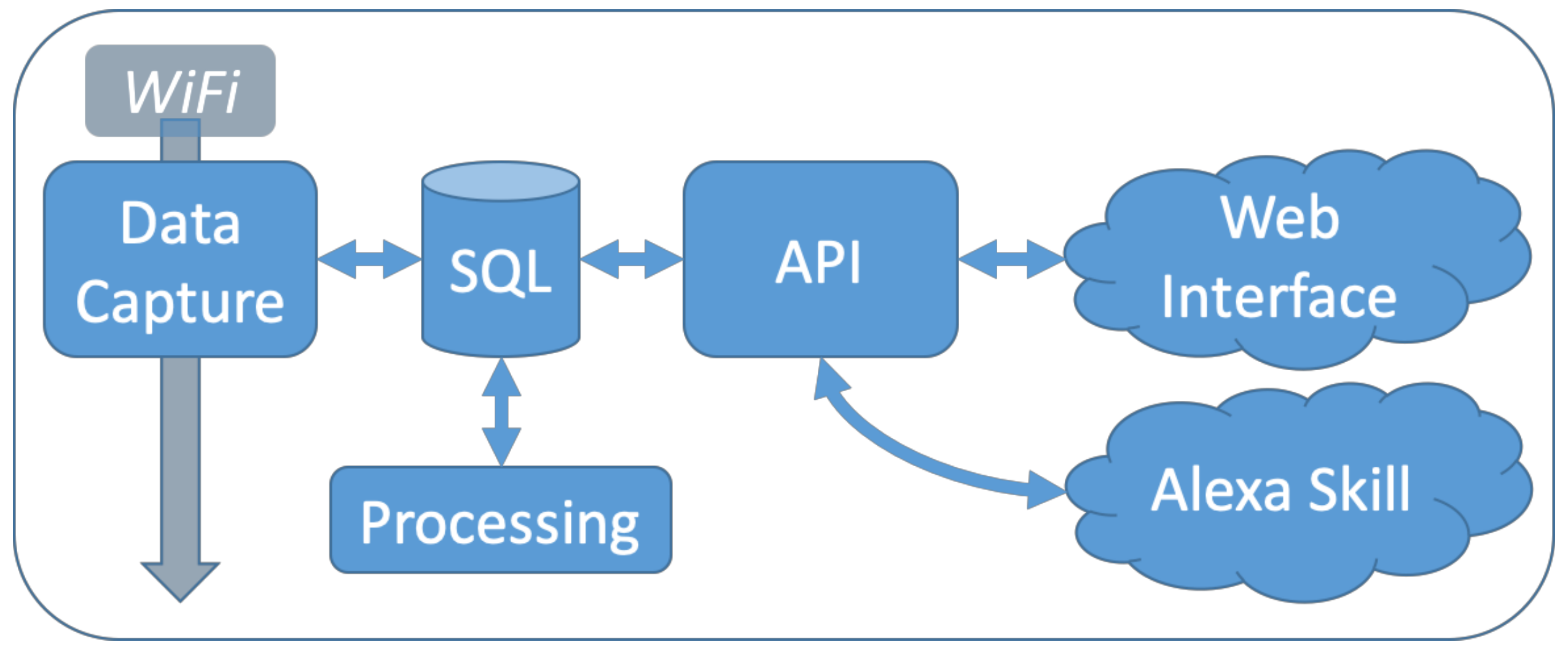
Exploring Data Flows in the Home



Data destinations by company and country

Aretha captures traffic meta data from devices connected to its WiFi hotspot, collating these with information about the companies and countries that data is transferred to. Aretha also re-identifies device behaviour from encrypted network traffic, showing users information their devices might inadvertently be leaking.

Analysis from Aretha is accessed via a web interface based on X-Ray Refine [3] and an Alexa skill supporting verbal reasoning about network traffic. This allows Aretha to 'retrofit' existing devices for more accessible interaction, allowing users to make assisted security and privacy decisions about their devices.



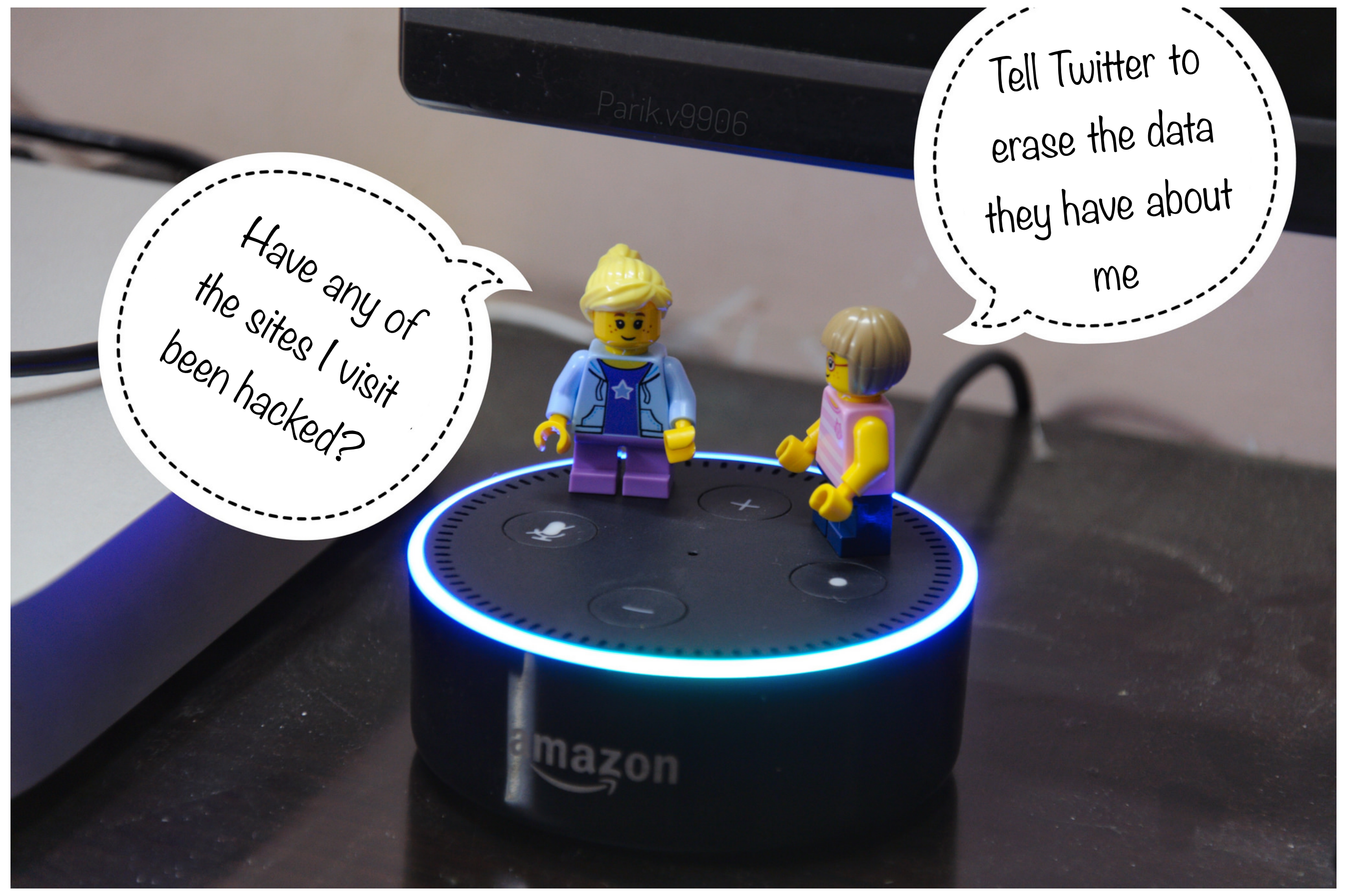
Data destinations by company and country

What If Your Firewall Could Talk?

The Aretha voice interface attempts to bridge the gap between the complex data understood by firewalls (e.g. ports and IP addresses) and human concepts used to make decisions (e.g. company names). Conversations with Aretha are designed to easily map these semantic concepts to logical constructs (e.g. “Google LLC” to 64.233.160.0/19).

Users are also able to engage in a form of Socratic dialogue with Aretha, providing the type of conversations about security and privacy that are missing from the smart home. These interactions accommodate the idiosyncratic nature of privacy preferences by providing users an opportunity to form informed preferences and develop them over time as circumstances change.

In this way, Aretha handles the repetitive tasks required for analysis, such as aggregating logs, allowing users to deal with unusual scenarios (as determined by device data flow models) with less mental fatigue.


Have any of the sites I visit been hacked?
Tell Twitter to erase the data they have about me

Sample Conversation: The Smart Firewall
Featuring the *User* and *Aretha*

A: Do you think your current devices send data to advertisers?
U: Yeah, probably
A: What about your Nokia Body scales, do you think they send health data, like your weight, to advertisers?
U: I guess?
A: Is this fine too?
U: Hmm, I think I'd rather it didn't do that
A: OK, Would you like me to block advertising traffic to and from the Nokia Body scales?
U: Yes please
A: Will do, let me know if this causes any problems

Evaluation
As part of the PETRAS IoT in the Home demonstrator, a prototype version of Aretha has been installed in a fully equipped smart home at the Building Research Establishment in Watford, UK. Future work will focus on the ability of IoT Refine to assist users in making security and privacy related decisions, as well as choosing between devices. An evaluation of the Refine interface itself is provided in [3].

Initial results using Aretha suggest that shifting the focus of VAs can lead to gains in home network security and privacy. Additional work on voice interactions shows the huge potential of future systems grounded in Aretha's distinctly human terms and concepts to assist users in gaining situational awareness of their home networks.

CENTRE FOR DOCTORAL TRAINING in CYBER SECURITY
EPSRC Engineering and Physical Sciences Research Council

[1] Reeves, B., and Nass, C. The media equation. Cambridge university press, 1996. [2] Van Kleek, M., et al. X-ray refine: Supporting the exploration and refinement of information exposure resulting from smartphone apps. CHI '18. ACM, 2018. [3] Shklovski, I., et al. "Leakiness and creepiness in app space: Perceptions of privacy and mobile app use." CHI '14 . ACM, 2014. [4] Zeng, E., et al. "End user security & privacy concerns with smart homes." SOUPS '17. USENIX, 2017.

Image credit, top to bottom: Rafa Garcés (CC/BY), Unknown (CC/BY), BRE Group (© 2014). All images used with permission.