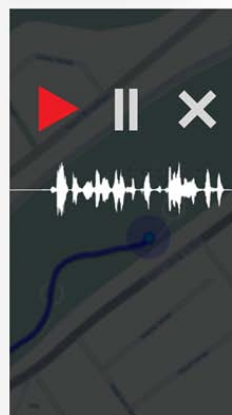
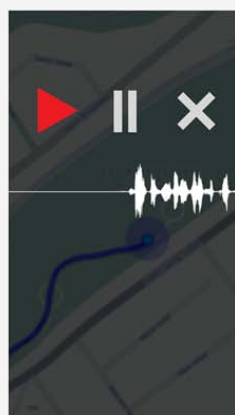
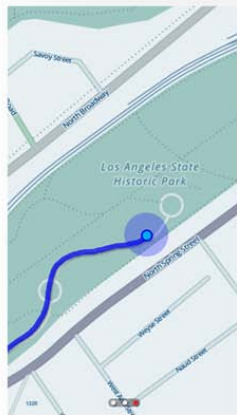
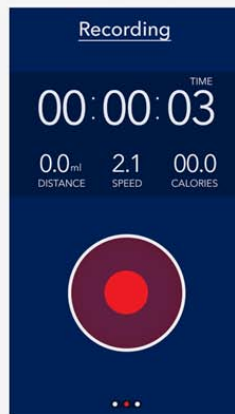
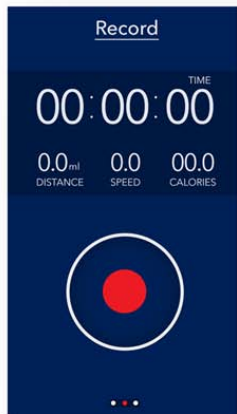


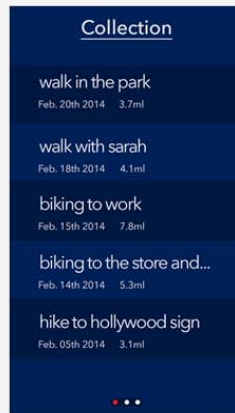
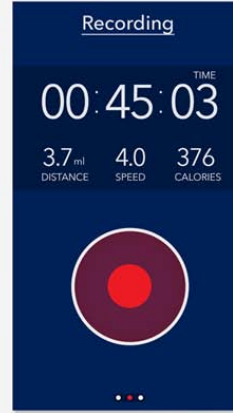
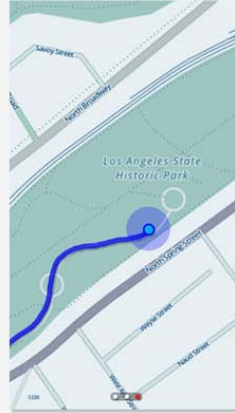
User Experience Research & Design for NDN mHealth & Identity Manager App



image source: Harrell Fletcher

Dustin O'Hara
Feb 2015
UCLA





NDN UX FLOW

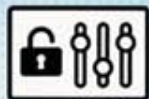


id manager



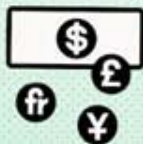
modem/isp

/user-namespace



data vault

payment



mHealth Fitness App
& other 3rd party apps



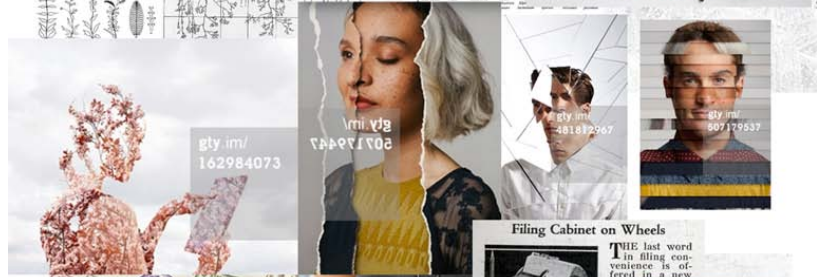
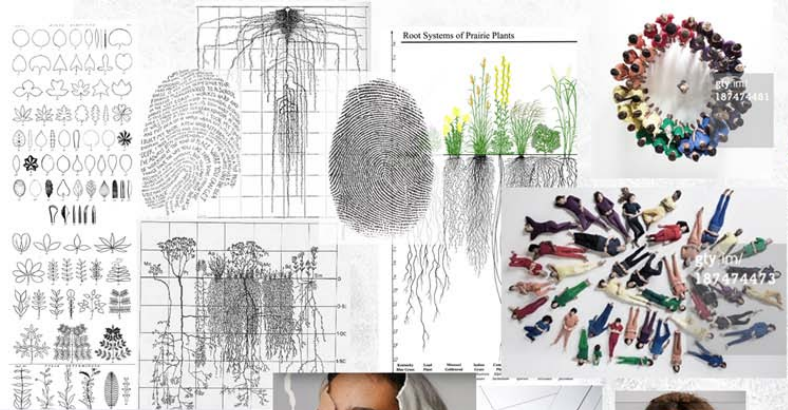
record activity



review activity data

storage

processing



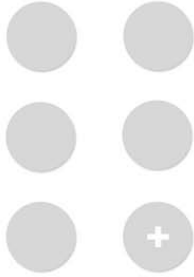
Filing Cabinet on Wheels

THE last word in filing convenience is offered in a new revolutionary file cabinet. It is placed in any office, and it is the only filing cabinet that plays a part in the success of your business. Manufacturers claim the system is speedy.

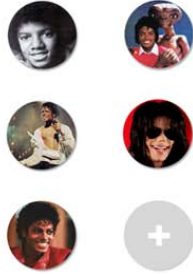
Carburetor attached to control ring.



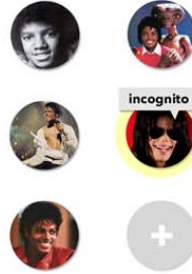
ID Manager



ID Manager



ID Manager



ID Manager



fitness

anonymous

payment_ID

auto_pay

family

social

ID Manager



fitness

anonymous

payment_id

auto_pay

family

social



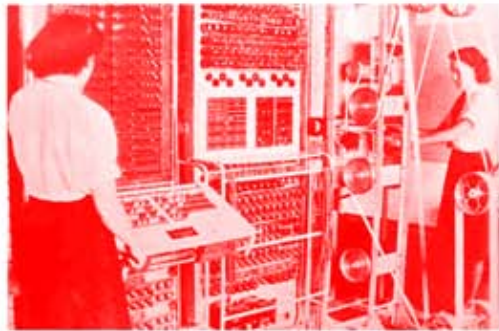


nations / armies / corporations



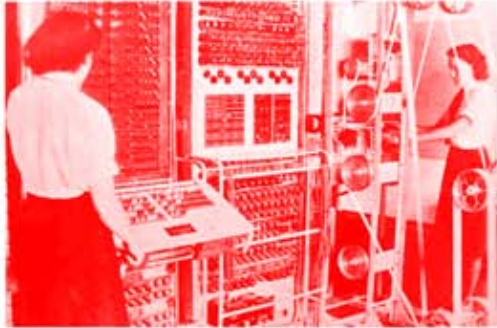
PKI

the individual





nations / armies / corporations



PKI

the individual

Why Doesn't Jane Protect Her Privacy?

Karen Renaud¹, Melanie Volkamer², and Arne Renkema-Padmos²

¹ School of Computing Science, University of Glasgow, Glasgow, UK
karen.renaud@glasgow.ac.uk

² CASED / TU Darmstadt, Hochschulstraße 10, 64289, Darmstadt, Germany
name.surname@cased.de

Abstract. End-to-end encryption has been heralded by privacy and security researchers as an effective defence against dragnet surveillance, but there is no evidence of widespread end-user uptake. We argue that the non-adoption of end-to-end encryption might not be entirely due to usability issues identified by Whitten and Tygar in their seminal paper “Why Johnny Can’t Encrypt”. Our investigation revealed a number of fundamental issues such as incomplete threat models, misaligned incentives, and a general absence of understanding of the email architecture. From our data and related research literature we found evidence of a number of potential explanations for the low uptake of end-to-end encryption. This suggests that merely increasing the availability and usability of encryption functionality in email clients will not automatically encourage increased deployment by email users. We shall have to focus, first, on building comprehensive end-user mental models related to email, and email security. We conclude by suggesting directions for future research.

Keywords: email, end-to-end encryption, privacy, security, mental model.

1 Introduction

Email was introduced in MIT’s CTSS MAIL around 1965 [46]. At this point privacy was not a primary concern. Subsequently, STARTTLS [36,25] led to the deployment of opportunistic transport layer encryption for email transmission. Recently, more email providers have started applying it by default, effectively protecting email privacy in transit. However, email providers themselves, and those who might be able to hack into the email servers, have full access to our email communication. *End-to-end* (E2E) encryption by end-users would protect emails from access by email providers and hackers too. Facilitating tools are readily available, including PGP/OpenPGP [4,10,9], PEM [30,31,32,33], MOSS [13], PKCS#7 [26], and S/MIME [39,40,41] according to Davis [14]. However, they generally have minimal real-world application outside of specific use cases.

The “Summer of Snowden” [23] has put digital security back in the limelight, and there has been a slew of new proposals for facilitating E2E encrypted secure messaging (e.g. DarkMail, LEAP, Pond, Mailpile, Brair), but there is, as yet, little evidence of mass uptake of E2E email encryption. The question that remains is “*Why is the use of end-to-end email security so limited?*” Previously, the poor usability of E2E encryption tools was advanced as the most likely explanation [50,44]. However, usability has improved

2. They are aware of the possibility of privacy violation of their emails but do not take any action for a variety of different reasons, perhaps because it does not *concern* them.
3. They know that the privacy of their emails can be violated but are not aware that this can happen in transit or at the mail server side. They may subsequently attempt to protect themselves against client-based threats, but *do not use E2E encryption*.
4. They know that the privacy of their emails can be violated in transit or at the mail server side but they *do not take any action* because they fail to see the need to act.
5. They know that the privacy of their emails can be violated (transit/server) and they want to prevent this but they *do not know how* to protect their emails against these types of threats, i.e. that they should use E2E encryption. They lack the knowledge, or have only partial knowledge.
6. They are concerned that the privacy of their emails can be violated (transit/server) and they understand that they can use E2E encryption to prevent this, but they *can’t* do it.
7. They are concerned that the privacy of their emails can be violated and they understand that they can use E2E encryption to prevent this, and they are able to do it, but still they have reasons not to — *they get side-tracked for some or other reason*.

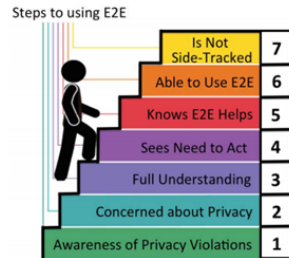


Fig. 1. Progression Towards E2E Encryption Deployment

For each of these explanations we will examine the relevant research literature and statements made by the participants in our study to see whether each is supported or challenged.

3 The Study

We performed an exploratory study consisting of semi-structured interviews, and subsequent qualitative analysis in order to identify users’ mental models of email security

Steps to using E2E

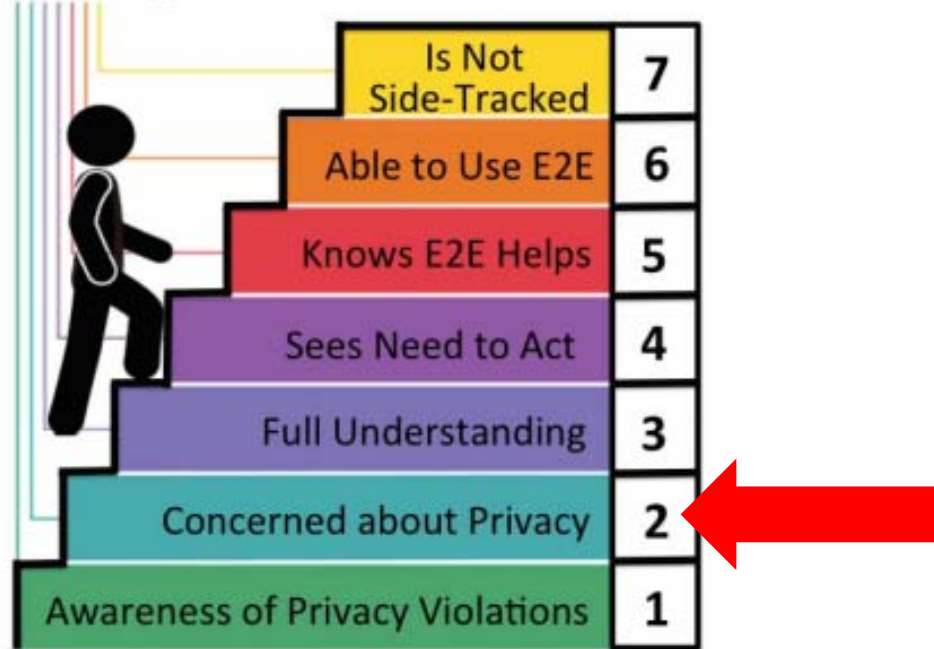
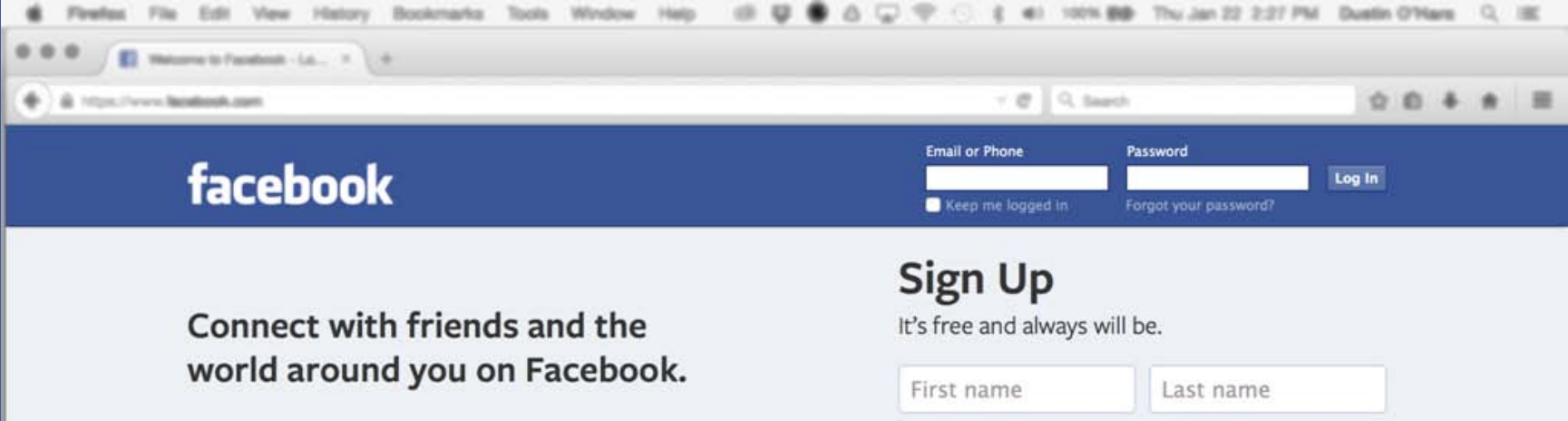


Fig. 1. Progression Towards E2E Encryption Deployment

“People want privacy, but they don’t want to practice privacy...” - Jean-François Blanchette



according to Google

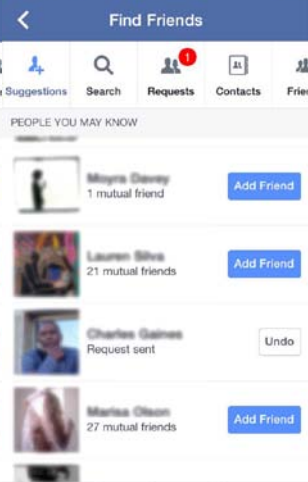
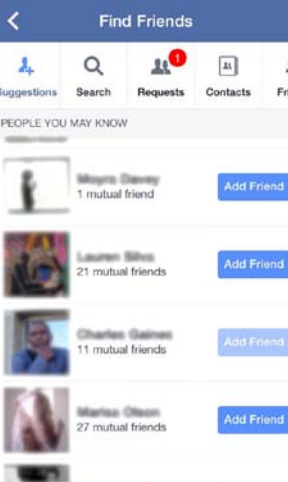
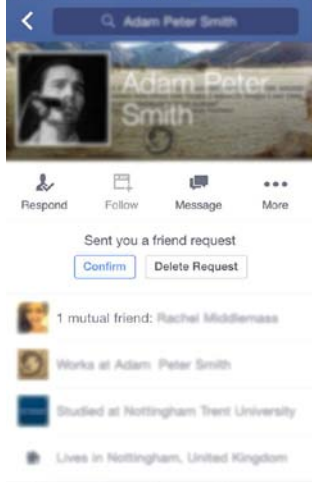
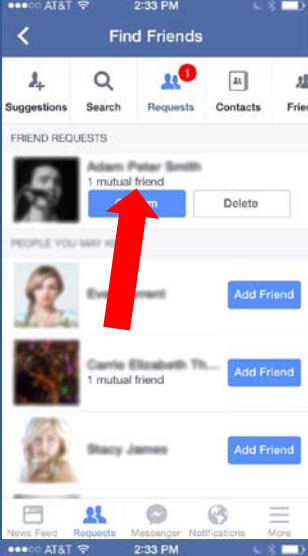
**Out of the 2.92 billion internet users,
roughly 42% of them are on facebook**

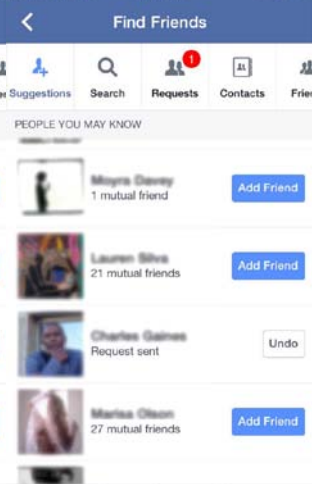
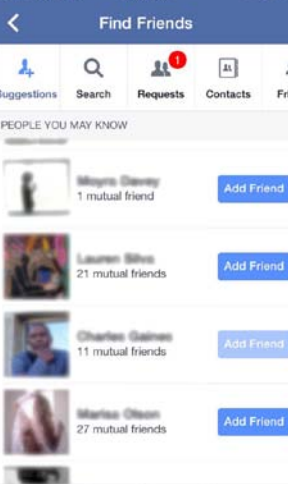
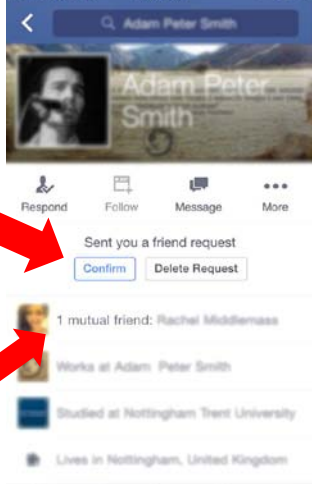
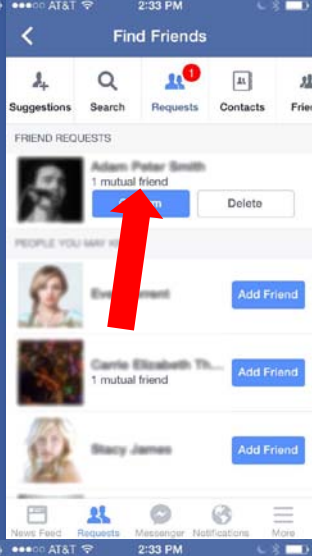
Female Male

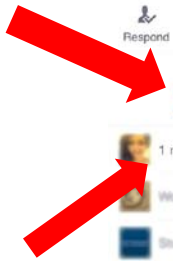
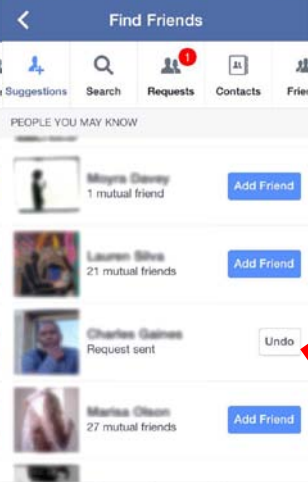
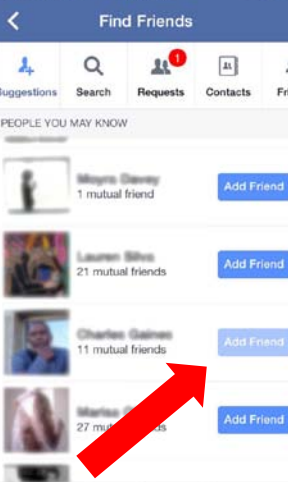
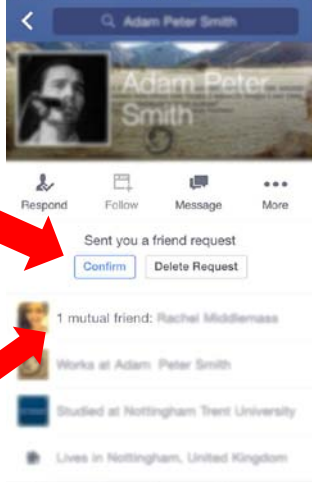
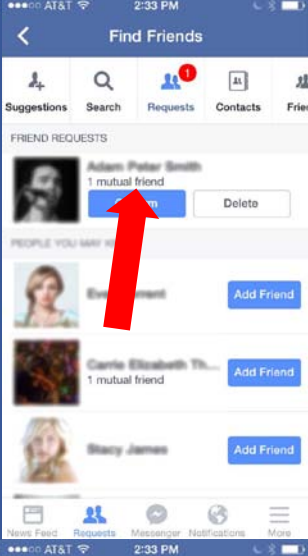
By clicking Sign Up, you agree to our [Terms](#) and that you have read our [Data Use Policy](#), including our [Cookie Use](#).

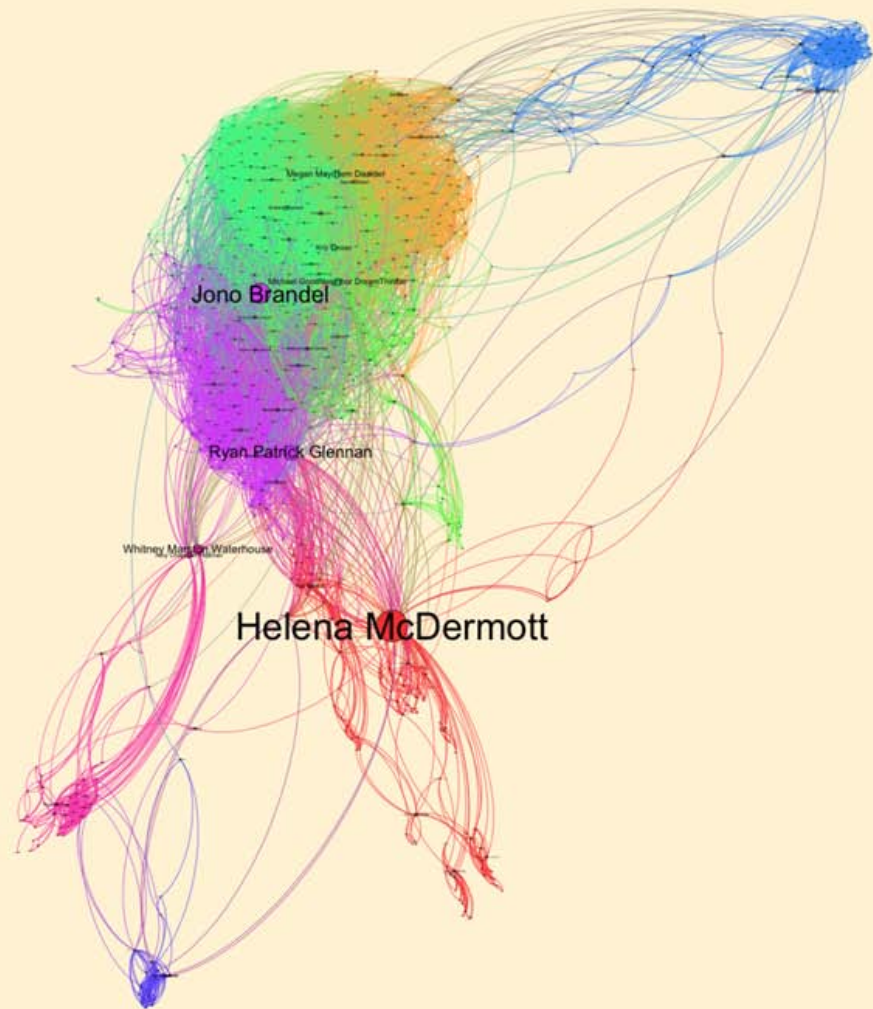
Sign Up

[Create a Page](#) for a celebrity, band or business.





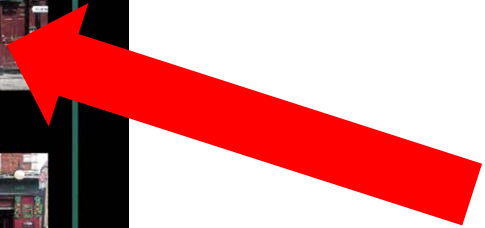




Articulating one's place within the network is often foundational to social practices involving trust.



BANK
OF
IRELAND
—
WAY OUT



DUBLIN PUBS

The ID Manager is about the management of context & trust (which then informs who gets access to public keys)

Trust & context are first established by situating and understanding one-another's place within the network, which is mirrored by the nature of the exchange.

ID Manager UX Ontology

- **numerous self defined identities**
 - **users**
 - **apps**
 - **data types**

Identities: enable to the user to quickly cluster their tasks, into self described categories or identities, (i.e. home & utilities, family, work, social, media, etc) that are each defined by the particular networking of users, apps, and data types.

Data Types: allow the user to quickly understand what data, or public keys, the various apps and users have access to. Rather than managing specific public keys, the user authorized clusters of public keys, for present and future exchanges.





Users: are understood as other individuals or groups that the user is actively, or potentially, exchanging data with. When authorizing a connection with a user, or reviewing existing connections, users are understood by their “mutual apps,” their “mutual users,” and the “data types” associated with their mutual apps.

Apps: function as form of trusted context for a given exchange, and are understood by their necessary “data types” and "mutual users.” Apps are identify and associate with a wider range of institutions and groups.

REQUESTS





 **Adam Tomas Jones**  
3 mutual apps / 11 mutual friends

[Confirm](#) [Delete](#)

 **LAHSP Fitness App**   
17 mutual users

[Confirm](#) [Delete](#)




SUGGESTED




   
Eva Torrance [Add User](#)
5 mutual apps
14 mutual users

  
Alice Room [Add User](#)
3 mutual apps
12 mutual users

  
Dana Mann [Add User](#)
4 mutual apps

REQUESTS





 **Adam Tomas Jones**  
3 mutual apps / 11 mutual friends

   LASHP Fitness...
Messenger, Spotify...

Authorize Secure Data Keys





   *fitness data key, exp 1/02/17*
messaging data key, exp 1/02/17




Confirm Delete

 **LASHP Fitness App**   
17 mutual users

Confirm Delete

SUGGESTED

   
Eva Torrance [Add User](#)
5 mutual apps
14 mutual users



Adam Tomas Jones

3 mutual apps / 11 mutual friends



David Delama

5 mutual apps / 33 mutual friends



Janet Owen

4 mutual apps / 21 mutual friends



Thomas O'Hara

8 mutual apps / 15 mutual friends



Eric Ablone

3 mutual apps / 4 mutual friends



Kathie O'Hara

3 mutual apps / 18 mutual friends



Requests



Users



Org / Apps



Data



Search



LASHP Fitness App
1 mutual app / 17 mutual users



LASHP Fitness Viz App
1 mutual app / 15 mutual users



Kaiser Permanente Thr..
2 mutual app / 51 mutual users



Sleep Cycle
1 mutual app / 13 mutual users








Venmo
1 mutual app / 107 mutual users














LA Department of Wat...
1 mutual app / 281 mutual users








HEALTH


 **LASHP Fitness App**
1 mutual app / 17 mutual users
   

 **LASHP Fitness Viz App**
1 mutual app / 15 mutual users
   

 **Kaiser Permanente Thr..**
2 mutual app / 51 mutual users
    

 **Sleep Cycle**
1 mutual app / 13 mutual users
   

HOME

 **LA Department of Wat...**
1 mutual app / 281 mutual users
