knowme

PIM
Personal Information
Management Ltd

CONFIDENTIAL

AGENDA

- Why Privacy by Design?
- Why and What is KnowMe
- Application of PbD Principles to KnowMe
- Key take outs
- Discussion

WHY PRIVACY BY DESIGN?

"Personal data is the new oil of the Internet and the new currency of the digital world."

Meglena Kuneva, European Consumer Commissioner

"On average an individual releases over 700 items of personal data per day to organisations and other individuals."

Venture Beat – February 2012

Gartner Says by 2019, 90 Percent of Organizations Will Have Personal Data on IT Systems They Don't Own or Control

- PIM is a member of the Personal Information Ecosystem Consortium (PDEC)
- PDEC actively worked with Ann Cavoukian as principles were developed
- We are focused in the area of Personal Information Management and our service must be trusted
- Principles are just common sense and a good guide for Architects and Solution Designers

WHY AND WHAT IS KNOWME

WHY

Value of Personal Information

Most system are not user centric

More system – more headaches

Maintaining data a head-ache for all

Cloud and mobile present opportunity for real user centric and user controlled systems

We hear of breaches all the time

A security or privacy breach would be a major issue for us

What

Mobile App and Cloud based Digital Vault "Owned" by the User

Personal Contact Mastering

User controlled sharing to individuals and organisations

Automatic updating of changes

Will evolve to include greenID and other Identity attributes

Launching iOS version early June

We designed KnowMe from the bottom up with Privacy by Design in mind.

1. PROACTIVE NOT REACTIVE; PREVENTATIVE NOT REMEDIAL

The Privacy by Design (PbD) approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen. PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred — it aims to prevent them from occurring. In short, Privacy by Design comes before-the-fact, not after.

- It is the persons data, they control who they share it with
- Full encryption with the individual holding the key – we cannot see the data
- There is only one "you" and the service is for you alone
- We would say PbD is the only way to design systems to be secure / private
- Early security architectural intervention is key early in systems design otherwise it will cost you a lot more later
- Ambulance at the top of the cliff not the bottom

2. PRIVACY AS THE DEFAULT SETTING

We can all be certain of one thing — the default rules! Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy — it is built into the system, by default.

- Base KnowMe settings are set to no sharing of data
- Only when an individual consents, is the data shared
- Lots of trade offs in design
- How do we treat privacy appropriately?
- E.g. Look to keep data on the phone
- Only upload data the user gives us permission to access

3. PRIVACY EMBEDDED INTO DESIGN

Privacy by Design is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.

- Set Architectural Principles for PIM including Privacy
- Privacy Policy
- These were core to design approach
- Sounds easy? There were challenges / trade offs
- E.g. Search? If we want to search across the system how do you do this if all info is encrypted?
- Privacy and security were put ahead of other factors to ensure trust in the service

4. FULL FUNCTIONALITY — POSITIVE-SUM, NOT ZERO-SUM

Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum "win-win" manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. Privacy by Design avoids the pretence of false dichotomies, such as privacy vs. security, demonstrating that it is possible to have both.

- Again – not an easy thing to do
- To enable business activity you need to share information
- If all your data is locked down then this cannot happen
- If the user wants to share their data then it is enabled and the exchange occurs

- Can appreciate there are many frustrated Architects out there ☺

5. END-TO-END SECURITY — FULL LIFECYCLE PROTECTION

Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved — strong security measures are essential to privacy, from start to finish. This ensures that all data are securely retained, and then securely destroyed at the end of the process, in a timely fashion. Thus, Privacy by Design ensures cradle to grave, secure lifecycle management of information, end-to-end.

- E.g. What happens when a user wants to close their account?
- KnowMe "ForgetMe" option
- Deletes everything we have re that user
- Removes data from any accounts it is shared to
- Limits to control though (e.g. if the data has been shared to other systems)

6. VISIBILITY AND TRANSPARENCY — KEEP IT OPEN

Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify.

"If it is free you are the product"

- Our aim - What you see is what you get
- Working towards Privacy Commission to review KnowMe
- We use open standards for data exchange and security
- We will be open and publish interfaces etc. to others in this area so they know how our system works

7. RESPECT FOR USER PRIVACY — KEEP IT USER-CENTRIC

Above all, Privacy by Design requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric.

80 percent of mobile internet users were concerned about sharing their personal information with apps and services. (Attitudes to privacy study commissioned by mobile trade association)

- No corporate systems are "yet" really user centric
- They are designed primarily around your business processes
- Customers enter your system
- KnowMe is the users system
- Aim is to develop it to connect to corporate services to give users more control
- Control is one of the 4 guiding principles of the NZ Data Futures forum

KEY TAKE OUTS

What data is out there about me that is out of date / wrong and I have no control over?

Usability of privacy controls (Vs Facebook and Google)

Readability of Terms and Conditions

iOS vs Android and Windows

- PbD - Why would you design a system any other way?
- There are trade-offs to be made
- Easier to build on new systems – hard to retrofit to existing systems
- But, we can only design and control our service
- Once data from our service is passed to an organisation, we are reliant on their privacy controls
- To build trust across the system we all need to work together and adopt principles like these

DISCUSSION AND CLOSE

Ross Hughson

MD PIM Ltd

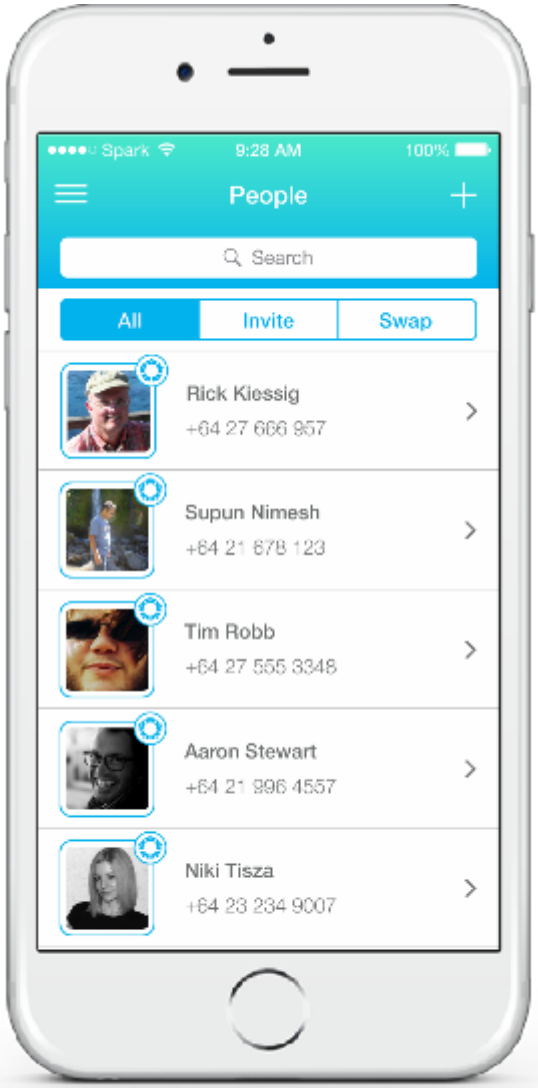
ross.hughson@knowme.nz

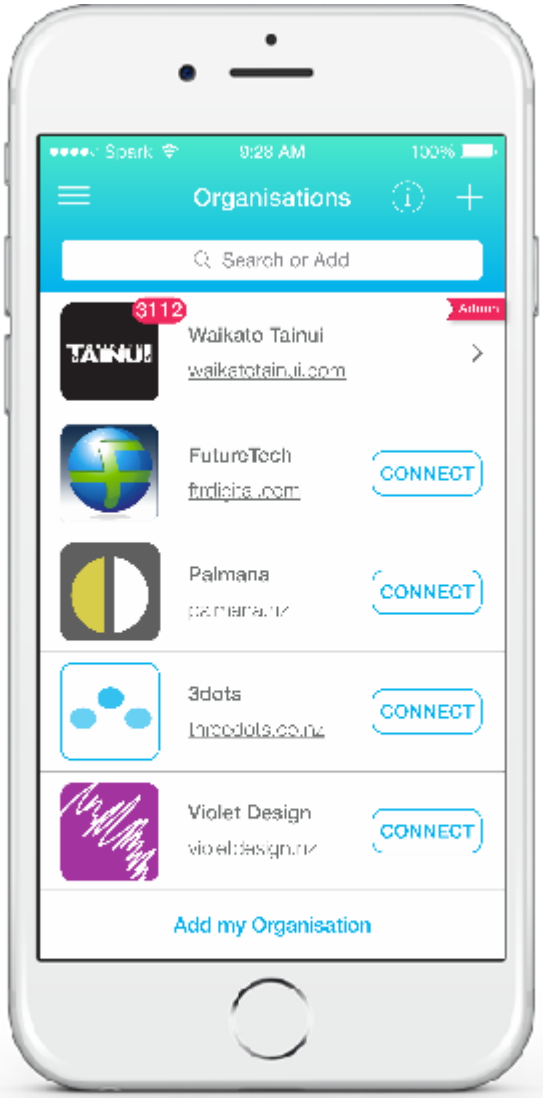
029 8902220

Discussion?

Questions?

NOTES PAGES


Spark
9:28 AM
100%
People
Search
All
Invite
Swap
Rick Kiessig
+64 27 666 957
Supun Nimesh
+64 21 878 123
Tim Robb
+64 27 555 3348
Aaron Stewart
+64 21 996 4557
Niki Tisza
+64 23 234 9007


Spark
9:28 AM
100%
Organisations
Search or Add
3112
Admin
Waikato Tainui
waikatotain.ui.com
FutureTech
CONNECT
Palmana
CONNECT
3dots
CONNECT
Violet Design
CONNECT
Add my Organisation

GSMA ARTICLE 2014

This time last year, a study of 11,500 users' attitudes to privacy commissioned by mobile trade association the GSMA found that over 80 percent of mobile internet users were concerned about sharing their personal information with apps and services.

So what's the mobile industry doing to win back consumers' lost trust? A panel on user-centric privacy at the MWC show in Barcelona, Spain this week discussed the need for a different approach to mobile - one that gives users transparency, choice, and control over their data by embedding privacy in products as they're developed.

Users know it. Correction: they should know it. Companies should too. But Mikko Hypponen, chief research officer at F-Secure, hammered the point home once again: "There are no free apps, no free cloud storage, no free webmail. They all end up monetizing one way or another," he told the panel on Monday.

'TRUST IS THE NEW CURRENCY': CAN THE MOBILE INDUSTRY WIN BACK USERS WITH PRIVACY PROMISES?

Summary:At this year's MWC, mobile execs have been mulling how best to balance consumers' right to privacy with the industry's hunger for data.

Data is the new currency of the digital world, broadcast and shared in real-time with devices that offer their users a better, healthier or more organised life. Yet, users are increasingly concerned about their personal information and how it's used by the tech companies they share it with. In fact, according to the GSMA, more than 80 percent of users (PDF) think it's important to have third parties ask for permission before accessing users' data.

As a result, "privacy is an important issue for all of us," Denelle Dixon-Thayer, SVP of business and legal affairs at Mozilla, said.

"We hear the ecosystem, but we really don't listen to what users are saying," she added, underlining the need for users to trust the web and mobile space in order "to get the most out of it".

ANTHEM SECURITY BREACH

http://www.wsj.com/articles/health-insurer-anthem-hit-by-hackers-1423103720

Anthem Inc., the country's second-biggest health insurer, said hackers broke into a database containing personal information for about 80 million of its customers and employees in what is likely to be the largest data breach disclosed by a health-care company.

Investigators are still determining the extent of the incursion, which was discovered last week, and Anthem said it is likely that "tens of millions" of records were stolen. The health insurer said the breach exposed names, birthdays, addresses and Social Security numbers but doesn't appear to involve medical information or financial details such as credit-card or bank-account numbers, nor are there signs the data are being sold on the black market.

More than listening

The industry knows it has to listen. But then what - how does it take what it's learned and put it to practical use? According to Claus Ulmer, group privacy officer at Deutsche Telekom, coding privacy-friendly products should be "a mandatory process for all developers". Brian Hernacki, chief architect at Intel, went a step further and called for platforms designed for privacy and technologies that automatically encrypt data, as "education, transparency, and accountability" are not enough.

Eduardo Ustaran, lawyer and partner at law firm Hogan Lovells International, echoed Hernacki's sentiment by highlighting how simply making information available may not help users become better informed. Most users don't read terms and conditions and privacy policies for the services they want to use because "they are too long", he said, and asked whether it's really worth writing them in the first place.

Instead, he called for a different legal approach "to create the right conditions to support innovation, and promote transparency and greater value sharing among data collectors".

Ustaran was also optimistic about the prospects for the European Commission to develop stricter regulation on how developers should handle the sensitive personal data that they're quietly amassing from all sorts of devices.

Some of the groundwork for that has already been laid. The article 29 Working Party, an independent EC advisory body on data protection and privacy, issued opinion 02/2013 (PDF) which details how the European legal framework applied to the processing of personal data in the development, distribution and usage of apps on smart devices and focuses on "the consent requirement, the principles of purpose limitation and data minimisation, the need to take adequate security measures, the obligation to correctly inform end users, the rights, reasonable retention periods and specifically, fair processing of data collected from and about children," Ustaran said.

Data protection vs privacy

But what does 'personal' really mean when it comes to data? And what does giving away personal data really imply? The moderator of the conference session, the GSMA's director of privacy Pat Walshe, believes that "privacy impactful information" would be a better term for such data.

The industry seems increasingly to believe that consumers will factor privacy into their buying decisions. Intel's Hernacki said that "data protection and privacy are not the same thing", adding that trust and reputation will become key factors in how users choose their tech providers.

Mozilla's Dixon-Thayer insisted that "data hygiene" should be something every new or established tech company should be thinking about. "Trust is the new currency," she said, even if it's hard to sell something just based on privacy outcomes alone. However things stand, Dixon-Thayer remains convinced that there is a real opportunity to use privacy as a competitive differentiator.

Future challenges

That potential will doubtless become more apparent as the internet of things grows - one estimate suggests there will be 50 billion connected objects in 2020 - gathering increasingly more sensitive data about our home lives and health. Wearables are "a totally different landscape for privacy", Hernacki said.

That's not to say that privacy and transparency and connected objects are mutually exclusive. Apple, for example, has been very clear to outline what can be done with users' health data in HealthKit - and when developers are stepping over the line. "Apple did it OK with the Health app, " said Mozilla's Dixon-Thayer.

The key to achieving real customer trust is to treat "customers as partners", Deutsche Telekom's Ulmer said. In the end, thinking about the issue of privacy as early as possible when setting up a new business or creating a service really shouldn't be that hard, the speakers agreed.

Read more on privacy

•Meet the free encryption app that promises to put your privacy first