Wearing My Heart on My Sleeve... Literally!

Barry Caplin

Tues. May 12, 2015, 11A
Wearing My Heart On My Sleeve... Literally!

Secure360
Tues. May 12, 2015
bcaplin1@fairview.org
bc@bjb.org @bcaplin
http://about.me/barrycaplin
http://securityandcoffee.blogspot.com

Barry Caplin
VP, Chief Information Security Officer
Fairview Health Services
Speaker. Geek. OpenSource. CISSP. CISA. CISM.

http://about.me/barrycaplin
securityandcoffee.blogspot.com
@bcaplin
Fairview Overview

• Not-for-profit established in 1906
• Academic Health System since 1997 partnership with University of Minnesota
• >22K employees
• >3,300 aligned physicians
  ▪ Employed, faculty, independent
• 7 hospitals/medical centers (>2,500 staffed beds)
• 40-plus primary care clinics
• 55-plus specialty clinics
• 47 senior housing locations
• 30-plus retail pharmacies

2012 data

5.7 million outpatient encounters
74,649 inpatient admissions
$2.8 billion total assets
$3.2 billion total revenue
Who is Fairview?

- Fairview Ridges Hospital
- Fairview Range Health Services
- Fairview Southdale Hospital
- Fairview Northland Medical Center
- Fairview Lakes Medical Center
- University of Minnesota Children’s Hospital
- University of Minnesota Medical Center
- Ebenezer
- PreferredOne
- Maple Grove Hospital
- Columbia Park Medical Group
- Institute of Athletic Medicine
- Minnesota Sports Medicine
Agenda

• WTF?
• Who’s Watching?
• You’re doing *what* with my data?
• You can’t see me… I’m anonymized!
• Security Challenges for home and work
Who’s got?...

“I asked you not to tell me that!”
Apr. 3, 2010

300K ipads
1M apps
250K ebooks
... day 1!

Toddler Buys Herself $50 Worth of iPad Apps
2011 – tablet/smartphone sales exceeded PCs
Apr. 24, 2015

1M orders
2500 apps available
... day 1!

The Apple Watch has arrived, and there are already over 2,500 apps jockeying for a place on your wrist.
2016 – IOT sales exceed smartphone+tablet

Global Internet Device Installed Base Forecast

BI INTELLIGENCE

Source: Gartner, IDC, Strategy Analytics, Machina Research, company filings, BII estimates
The Predicted Wearables Boom Is All About The Wrist

Worldwide wearable device shipment forecast (in million units)

- **Wristwear**
  - 2014: 17.7
  - 2015: 40.7
  - 2019: 101.4

- **Modular**
  - 2014: 1.6
  - 2015: 2.6
  - 2019: 6.7

- **Clothing**
  - 2014: 0
  - 2015: 0.2
  - 2019: 5.6

- **Eyewear**
  - 2014: 0.1
  - 2015: 1.0
  - 2019: 4.5

- **Earwear**
  - 2014: 0
  - 2015: 0.1
  - 2019: 0.6

- **Other**
  - 2014: 0.2
  - 2015: 1.1
  - 2019: 7.3

**Total shipments**
- 2014: 19.6m
- 2015: 45.7m
- 2019: 126.1m

Source: IDC
New smart devices don’t have to replace the smartphone.

Adoption rate of wearables parallels that of tablets.

20% of Americans in 2012 owned a tablet after just two years on the market

40% of Americans own a tablet today

21% of American adults already own a wearable device

? of American adults will own a wearable device in two years

76% of consumers say they would NOT need their wearable device to replace an existing piece of technology in order to justify its purchase.
Figure 3: Health tops list of information US consumers want from wearables
Consumers were asked what information they want to receive from wearable technology.

- Exercise smarter: 77%
- Collect and track medical information: 75%
- Eat better: 67%
- Finding retail deals: 46%
- Controlling home appliances: 32%
- Access to entertainment: 29%
- Plugging into social media: 26%

Source: HRI/CIS Wearables consumer survey 2014
High Hopes?

Consumers:
• Not yet embraced
• Don’t want to pay too much
• Skeptical about social sharing
• Concerned about Privacy
Who’s Watching?

2014 FTC report on Data Brokers

• Combine online & offline – often without consent
  - Purchases
  - Social Media
  - Warranty info
  - Subscriptions
  - Affiliations

• They share

• Analysis creates Inference

• Regulation proposed
Back To The Future!
Oh! the Places You'll Go!

You, the Patient

1997

Life Insurance Company

Employer (Yours, Spouse)

Payer (Insurer)

Consulting Physician

Pharmacy

Pharmacy Benefits Manager

Researcher

Employer's Wellness Program

Hospital

Accreditation

Law Firms

Vital Statistics
Example TOS/Privacy – Fitness device

• 13 or older
• Account with valid email
• Rules about posting content
• You own your content
• Use at your own risk
• Consult doctor before exercising
• “Use Common Sense”/Wear & Care – skin
• 3rd party disclaimer
• Indemnity
• Limitation of Liability/Dispute Resolution
Example TOS/Privacy – Fitness device

- Only collect data useful to improving products, services, experience
- Transparency
- Never sell PII (can opt-in)
- Take security seriously
- Info:
  - Email address, pw, nickname, dob
  - Oauth: name, profile pic, friend list, phone contact list (friend id – not saved)
  - Web logs incl. IP
  - Cookies – don’t honor DNT – AppNexus, DataXu, DblClick, Google AdWords, AdRoll, Twitter, LiveRamp, Advertising.com, Bidswitch, Facebook, Genome, SearchForce
  - Analytics – Mixpanel, Google Analytics, New Relic, KissInsights, Optimizely
  - Friends’ contact info
  - Location – GPS, WiFi APs, cell tower IDs
Example TOS/Privacy – Fitness device

• De-Identified data -> health community, marketing, for sale
• PII shared with:
  • Order fulfillment, email mgmt., CC processing firms
  • Legal or Gov’t request
  • Merger, sale or reorg
  • Anyone user specifies (third party apps)
65 billion
Location-tagged payments made in the U.S. annually

154 billion
E-mails sent per day

87%
U.S. adults whose location is known via their mobile phone

Digital Information Created Each Year, Globally

2,000% Expected increase in global data by 2020

III Megabytes
Video and photos stored by Facebook, per user

75%
Percentage of all digital data created by consumers

Sources: IDC, Radicati Group, Facebook, TR research, Pew Internet
Who’s Watching?

2014 FTC report on Data Brokers

• Combine online & offline – often without consent
  - Purchases
  - Social Media
  - Warranty info
  - Subscriptions
  - Affiliations

• They share
• Analysis creates Inference
• Regulation proposed
Data Brokers collect

- Basic ID data – name, address
- ++ – ssn, license #
- Demographics – A/S/L, race, employment, religion
- Court records – bankruptcy, criminal, domestic
- Home/Neighborhood – rent/loan info
- Interests
- Financial – credit, income, net
- Vehicle – brand, new/used
- Travel – preferences
- Purchase behaviors
- Health – tobacco, allergies, glasses, supplements
De-Identi-what?

• 2000 study – 87% census ID’d using: zip, d.o.b., gender

• 2013 – 40% of genome participants ID’d

• 2008 – 80% ID’d using when/how for 3 Netflix ratings
  http://ieeexplore.ieee.org/xpl/articleDetails.jsp?reload=true&arnumber=4531148

• Feb deal between Facebook, Acxiom and other data brokers
  – Acxiom data linked to 90% of US social profiles

• MIT – 4 phone position samples to link to specific person

https://epic.org/privacy/reidentification/ + MIT + UCLA
De-Identi-what?
(re-identification)
(De-anonymization)
Data Exfil

• Data explicitly given
• Implicitly but known (phone, Google Now)
• Implicitly but unknown

• Transitive Consent
Is Privacy Dead?

• Just the definition!
• Privacy is about control
• You must have the ability to decide:
  – What
  – When
  – How, and
  – With whom
  You share your personal data
• What’s in it for you
“Magic Quadrant” of Data Leak Pain

- Surprise
- Clueless
- Control
- Don’t Care

Unknown

How Much

Known

No/Yes

Huh?

Choice

Fairview
Future Shock

• Msoft/U of Rochester (NY)
• GPS + vehicle data
• Where you will be 80 weeks from now – 80% confidence

Security Challenges

- Exposure of data
- Leakage of data – sold, donated, tossed, repaired drives
- Poor Design/Protocols
- Malware
- Integrity
- Availability

But don’t we have all this now???
<table>
<thead>
<tr>
<th>Drawbacks: Percent of consumers who say wearable tech will...</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>...make us vulnerable to security breaches</td>
<td>86%</td>
</tr>
<tr>
<td>...invade my privacy</td>
<td>82%</td>
</tr>
<tr>
<td>...hurt our ability to relate to other humans</td>
<td>72%</td>
</tr>
<tr>
<td>...make me too dependent on technology</td>
<td>68%</td>
</tr>
<tr>
<td>...lead us all to own and use too many devices</td>
<td>65%</td>
</tr>
<tr>
<td>...take away my autonomy at work</td>
<td>54%</td>
</tr>
<tr>
<td>...turn us into robots</td>
<td>52%</td>
</tr>
<tr>
<td>...make my job unnecessary/redundant</td>
<td>47%</td>
</tr>
<tr>
<td>...make everyone look ridiculous</td>
<td>37%</td>
</tr>
</tbody>
</table>
At Work

Weart this biosensor so management can monitor your health during the day.

WOW. I didn’t know you cared so much about my health.

Oh, I do.

Employee 479 doesn’t have shallow breathing. You can give that one some more work.
At Work

• Wearable = portable = stealable
• What data
• How stored – device, phone, computer, component, cloud
• How backed up (cloud)
• Encryption available?
• Location
• Medical, health info on staff
• Additional info exposure – opportunities for social engineering
For Work?

• BYOW?
• Employer-provided?
  – Badge
  – Smartphone
  – Glass?
  – RTLS?
  – Health/fitness monitoring?
  – Time – Desk, Meetings, Bathroom, Break, Lunch or Coffee time?
Additional Attack Vectors

- Glasses or camera-enabled
  - Video/pictures
  - IP disclosure?
  - Glass-jacking?

- Info disclosure and “Bio-Social Engineering” ©
  - Accelerometer/Tempest
  - Negotiation biomarker disclosure – never let them see you sweat!
  - Human pattern mapping
  - Biomarker manipulation
  - Augmented Reality distortion
  - Group Movement/Behavior
KEEP CALM AND JUST SAY NO
Medical

- Quantified Self
- Insulin pumps, pace-makers, ICD, etc.
  - FDA requirements
  - Device manufacturers
  - Ease of connection
- Barnaby Jack, HackerHalted
  Jay Radcliffe, BlackHat
- Homeland attack (Broken Hearts, s2/ep10 12/2/12)
  - Wireless attack via pacemaker id/sn
  - Dick Cheney, 2007
- MITM or snooping
- Integrity
- Availability
• Primary mechanism is… Obscurity
• Focus is on
  – Function
  – Aesthetics
  – Communication
  – Cost
  – Speed to Market
• Testing?
• Patching?
• Design?
• Built-in or Bolted on?
• Encryption?
• Proximity?
• Policy – use; carrying; connections; physical locations
• NAC?
• Personal perimeter?
The **Real** Issue...
What will the wearable future look like?

52% of adults agree that automated facial recognition will replace the need to remember names.

56% say life expectancy will increase on average by 10 years.

42% agree that the average person’s athletic ability will improve dramatically.

52% say that half of all TV watching will happen on wearable screens.

46% say obesity rates will decrease.

52% agree that people will rarely have face to face conversations.

57% agree that people will rely more on their wearable devices for support than they do their friends & family.

55% agree that everyone will work from home/remote at least part of the time.

63% agree that work and life will become inseparable.
CISOs are from Mars

CIOs are from Venus

Secure360
Tues. May 12, 2015 1:30P
bcaplin1@fairview.org
bc@bjb.org @bcaplin
http://about.me/barrycaplin
http://securityandcoffee.blogspot.com

Barry Caplin
VP, Chief Information Security Officer
Fairview Health Services