Auditing moving targets:
Smartphones & tablets in government

– or –

a CISO-turned-auditor's

take on mobile devices

John Bullock, BSc, CISSP, CISA, CRISC, GICSP
Senior IT Audit Specialist
Office of the Auditor General of BC
jbullock@bcauditor.com / ca.linkedin.com/in/jb00seven

what's in it for you

- mobile device audit gotchas
- cybersecurity & privacy insights specific to mobile
- perspective of both security practitioner & auditor

what's in it for me

- mobile device enthusiast
- audit enthusiast

why mobile devices?

We use them for …

everything!

from 99 things replaced by smartphones

life recorders

diary, camera, video camera, audio recorder, …

organizers

watch, alarm clock, personal planner, social calendar, …

productivity

calculator, GPS navigation, compass, address book, dictionary, barcode scanner…

entertainment

music player, game console, radio, TV, remote control, …

reading

books, comics, recipes, magazines, newspapers, …

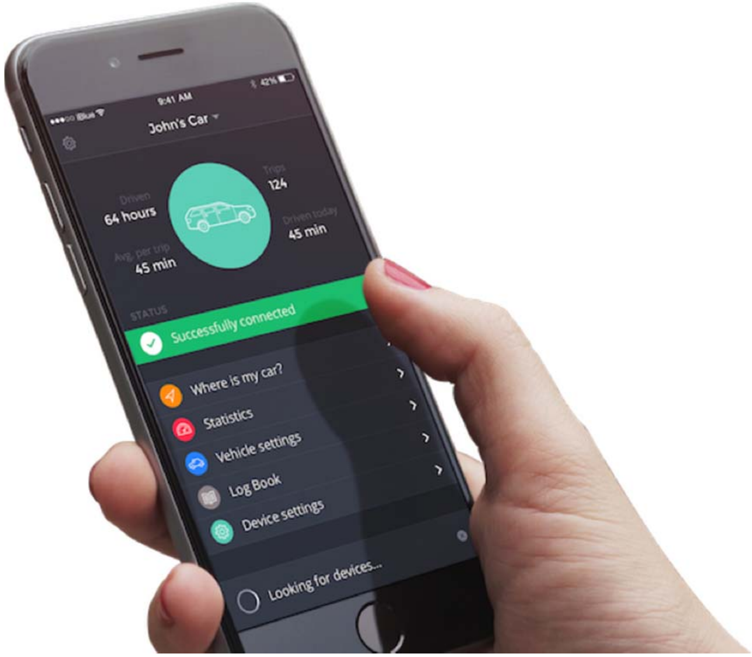
tools

flashlight, measuring tape, level, magnifier, telescope, …

CHIPOLO

1438

SCHLAGE
1 2 3
4 5 6
7 8 9
0
SCHLAGE


9:41 AM
John's Car
Driven
64 hours
Trips
124
Driven today
45 min
Avg. per trip
45 min
STATUS
Successfully connected
Where is my car?
Statistics
Vehicle settings
Log Book
Device settings
Looking for devices...

Immobilizer
Immobilizer
iBlue
Bluetooth

why an audit?

↑ functionality = ↑ risk

risk factors: size

- small size → high number of devices lost or stolen

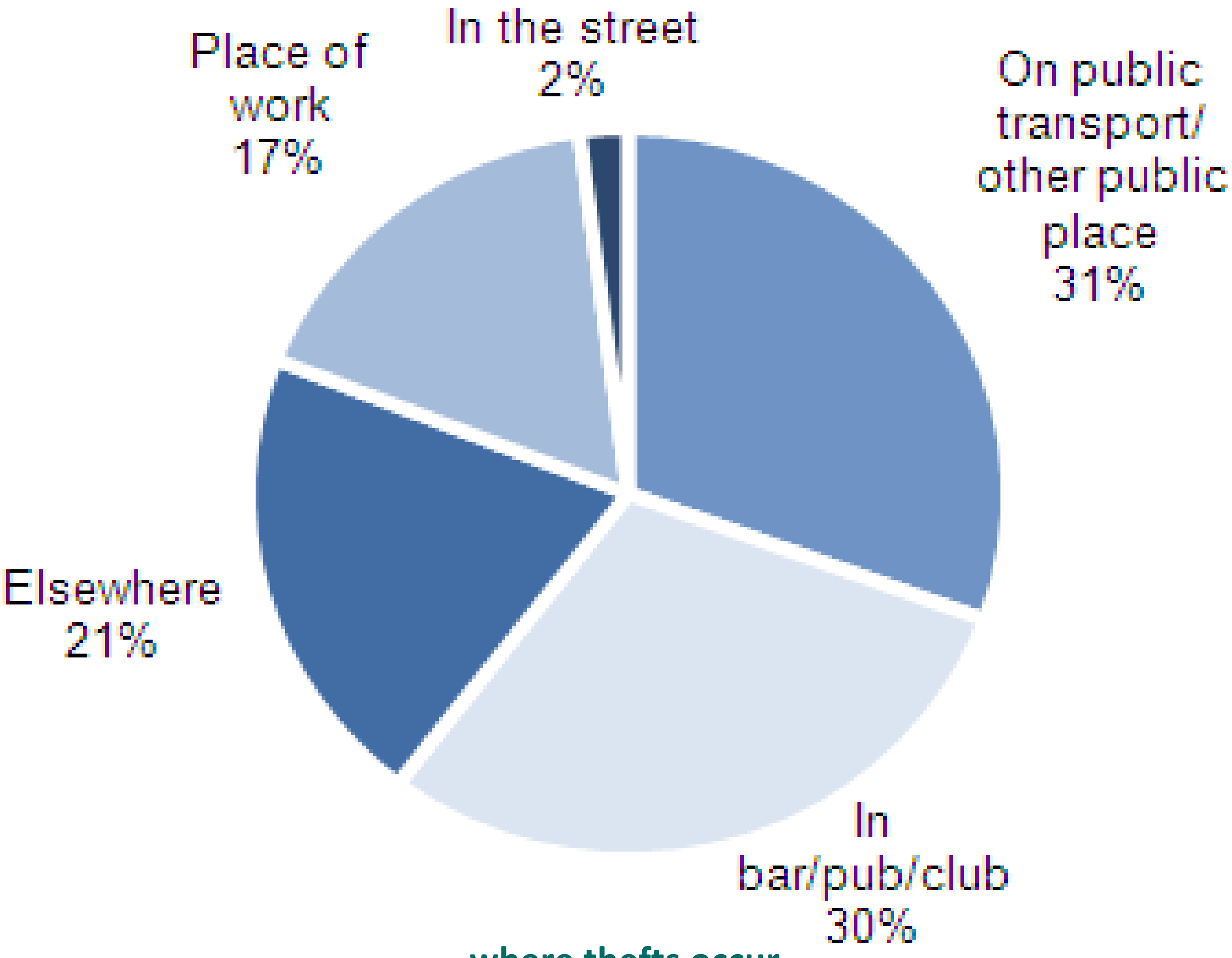
"One in 10 smartphone users have had their phones stolen"
http://www.wired.com/2014/12/where-stolen-smart-phones-go/

For lost-but-returned devices, more than 90% of the good Samaritans snooped before returning them
http://www.informationweek.com/mobile/lose-your-smartphone-finders-will-snoop-through-it/d/d-id/1103354

loss & theft

- 2.1m stolen
- 3.1m lost

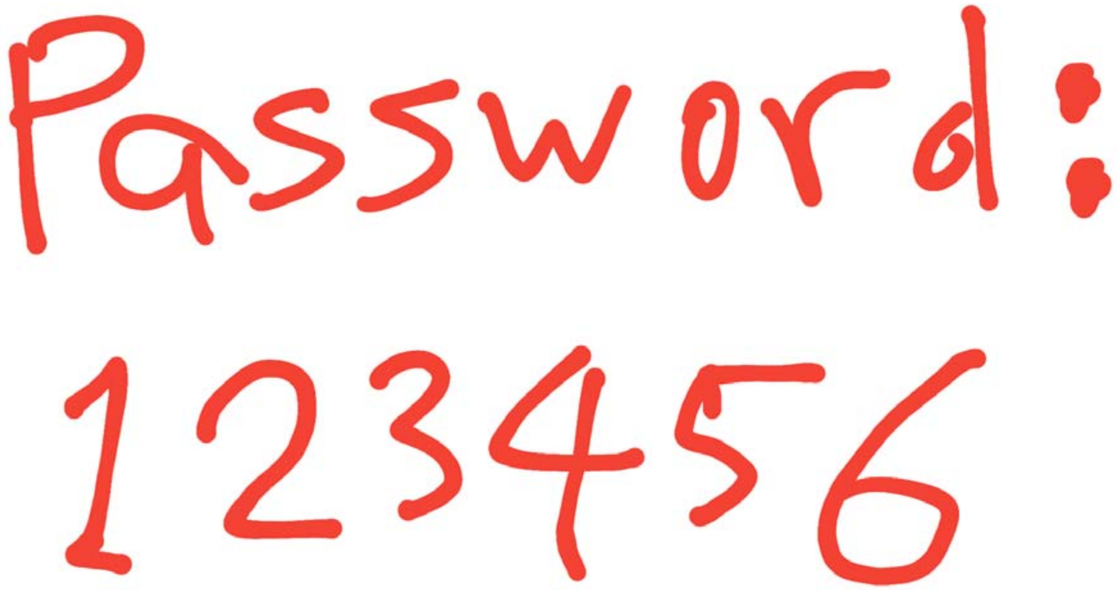
(stats taken from a 2015 US report)



where thefts occur

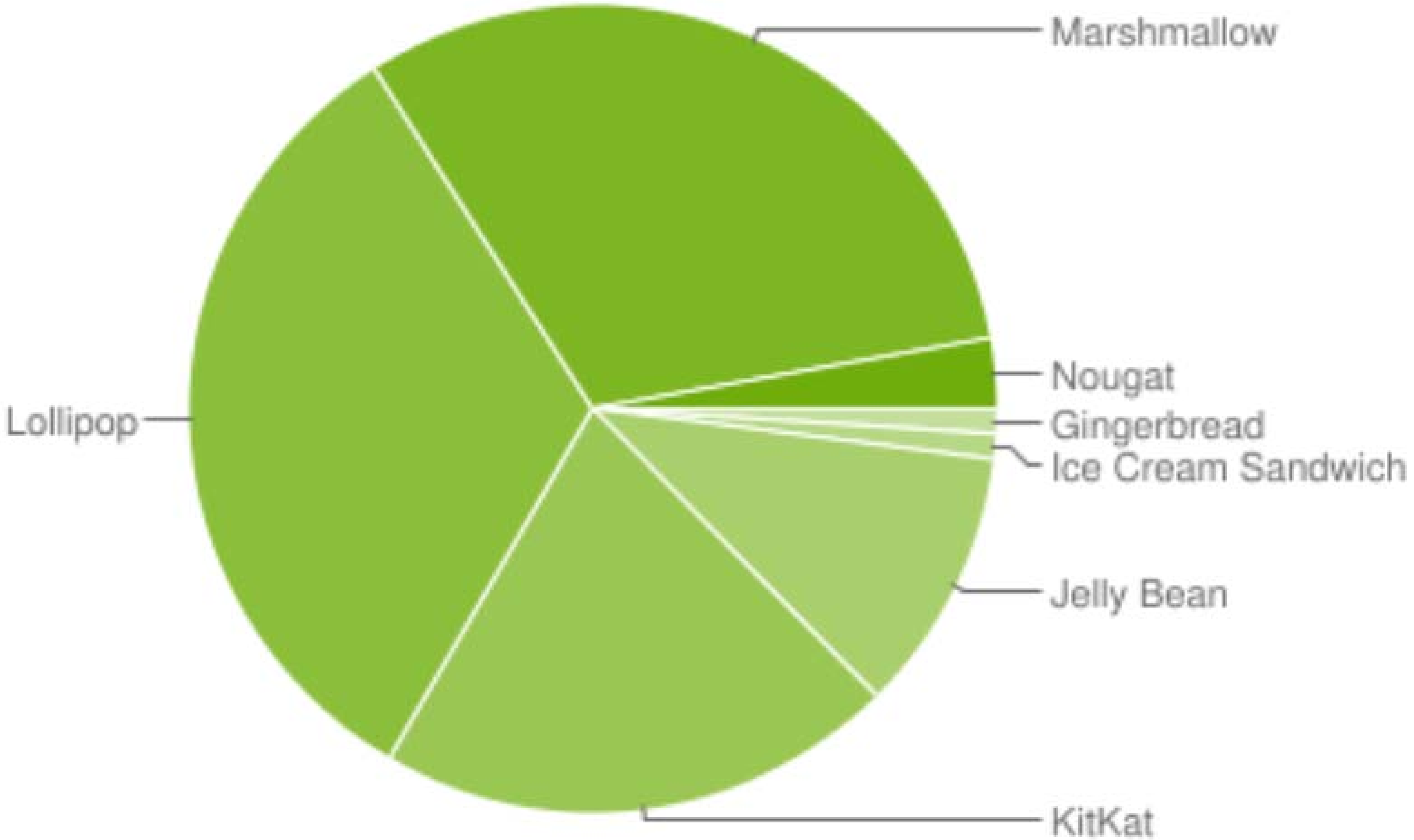
risk factors: keyboards/passwords

- tendency to use simple passwords due to the lack of a physical keyboard (or a very small keyboard)



risk factors: lack of support

- frequent model changes mean devices quickly become unsupported (can't get security updates)



risk factors: malware

- evolving operating systems provide opportunities for malware (**mal**icious soft**ware**)

New mobile malware tripled in 2015. Growth continued in 2016 with Ransomware (which blocks access until a user pays a sum of money) as the latest flavour. https://www.scmagazineuk.com/kaspersky-finds-significant-growth-of-mobile-malware-in-2015/article/531116/

how to start the audit?

Hello
my name is
~~Heisenberg~~ ?

names/words matter

What is a mobile device?

- flash drive?
- laptop?
- tablet?
- dumb (i.e. *feature*) phone, cell phone, smartphone?

Name of audit: MDM or MMD?

- *Mobile Device Management* is a product
- **Management of Mobile Devices** ✓
  - allowed for Policies, Procedures, Standards, Guidelines, and Practices.

What's in scope?

What's out of scope?

scoping

The big question: **laptop/tablet/smartphone**

Think: What's different?

- small input area (strong passwords more difficult)
- dramatically higher loss/theft risk
- immature security measures for OS/device

smartphones & tablets with mobile specific OS ✓

- **not** laptops (we know how to easily secure them, even if we don't)
- **not** flash drives, **not** even Chromebooks

The awkward question: BYOD

Depends on whether official BYOD program or not

Yes?

- May need to examine personal devices. Talk to a lawyer.

No?

- Whew. Examine controls to prevent, detect and remediate existence of BYOD devices. ✓

scoping

The easy question: privacy

The following are *largely* personal privacy issues:

- location information (current/past GPS coordinates, and Wi-Fi and Bluetooth connection histories
- photographs
- app behaviour (Best Flashlight & contacts)
- performance data (telemetry)
- voice commands

we scoped it out ✓

- resources constrained
- coordinated audit w/ Privacy Commissioner investigation!

scoping

Other questions:

- phishing
- mobile banking

Solution? Think, is it different on mobile?

- largely "NO"
- but be prepared to justify your decisions again & again

lines of enquiry

1. strategic planning activities

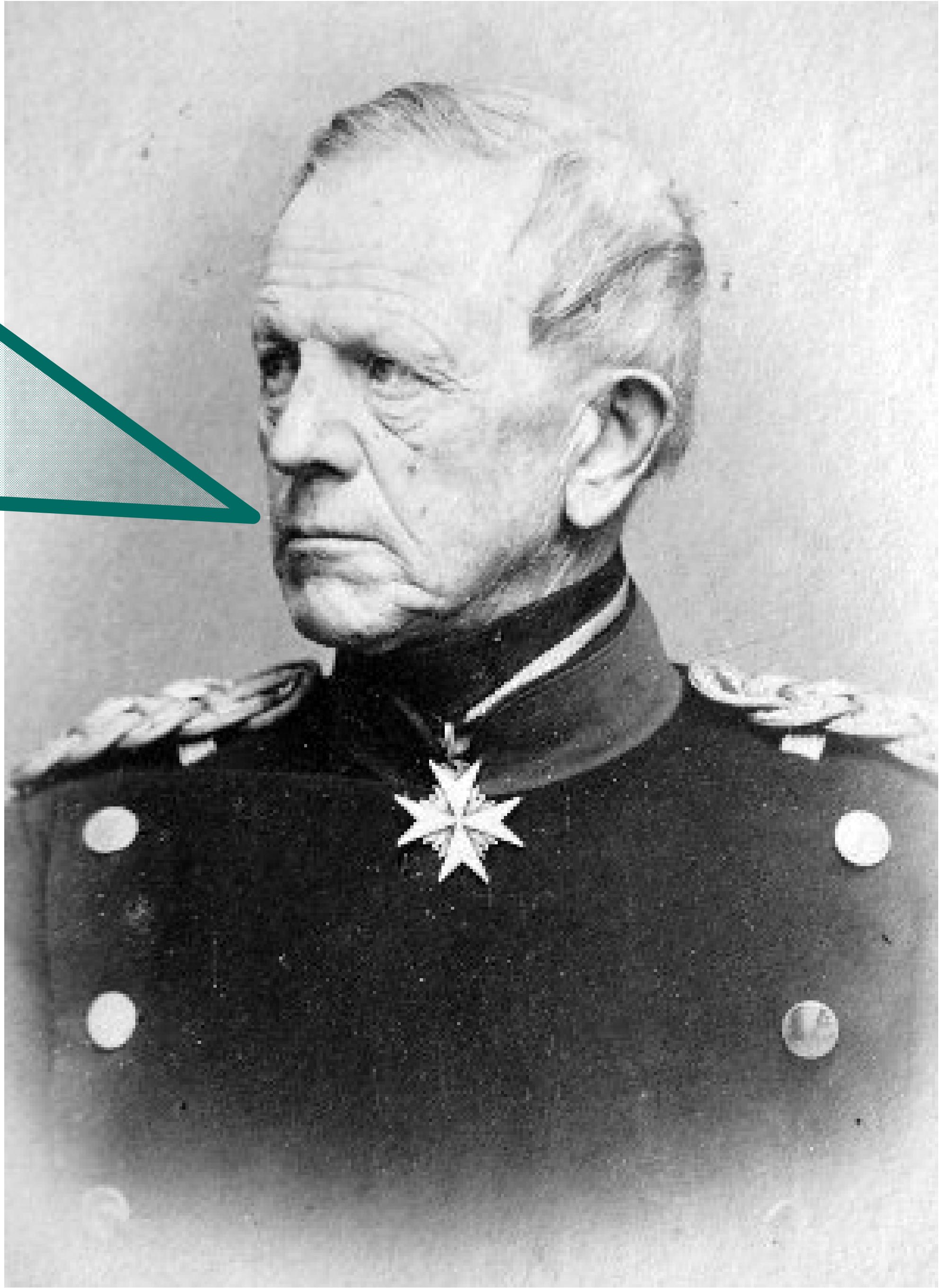
2. full lifecycle management of devices

3. security controls

4. monitoring, logging, incident management

No audit plan survives contact with the auditee.

~ Helmuth von Moltke, with apologies



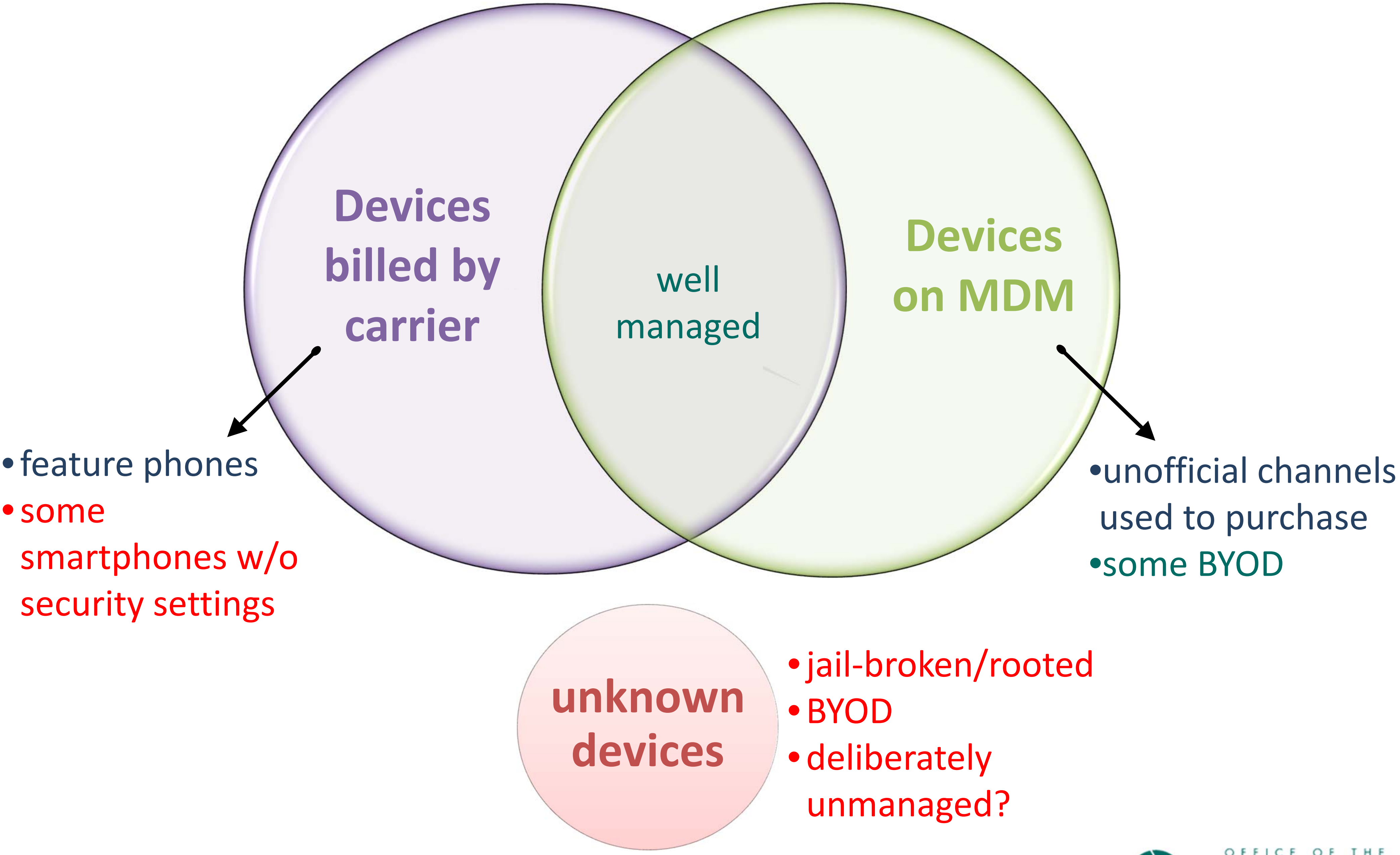
risk gotchas

- "Why does X matter? We/they can do remote wipe.
- "It's unreasonable for us/them to have to type a passcode several times a day."
- "Doesn't the fact that a smartphone is a *tracking device* cause security issues?"

Cause:

- infatuated with technology ☺
- mobile devices are the Most Personal Computers. Ever!
- confusing privacy and security / seeing only risk, not benefits

inventory gotcha



Devices billed by carrier

well managed

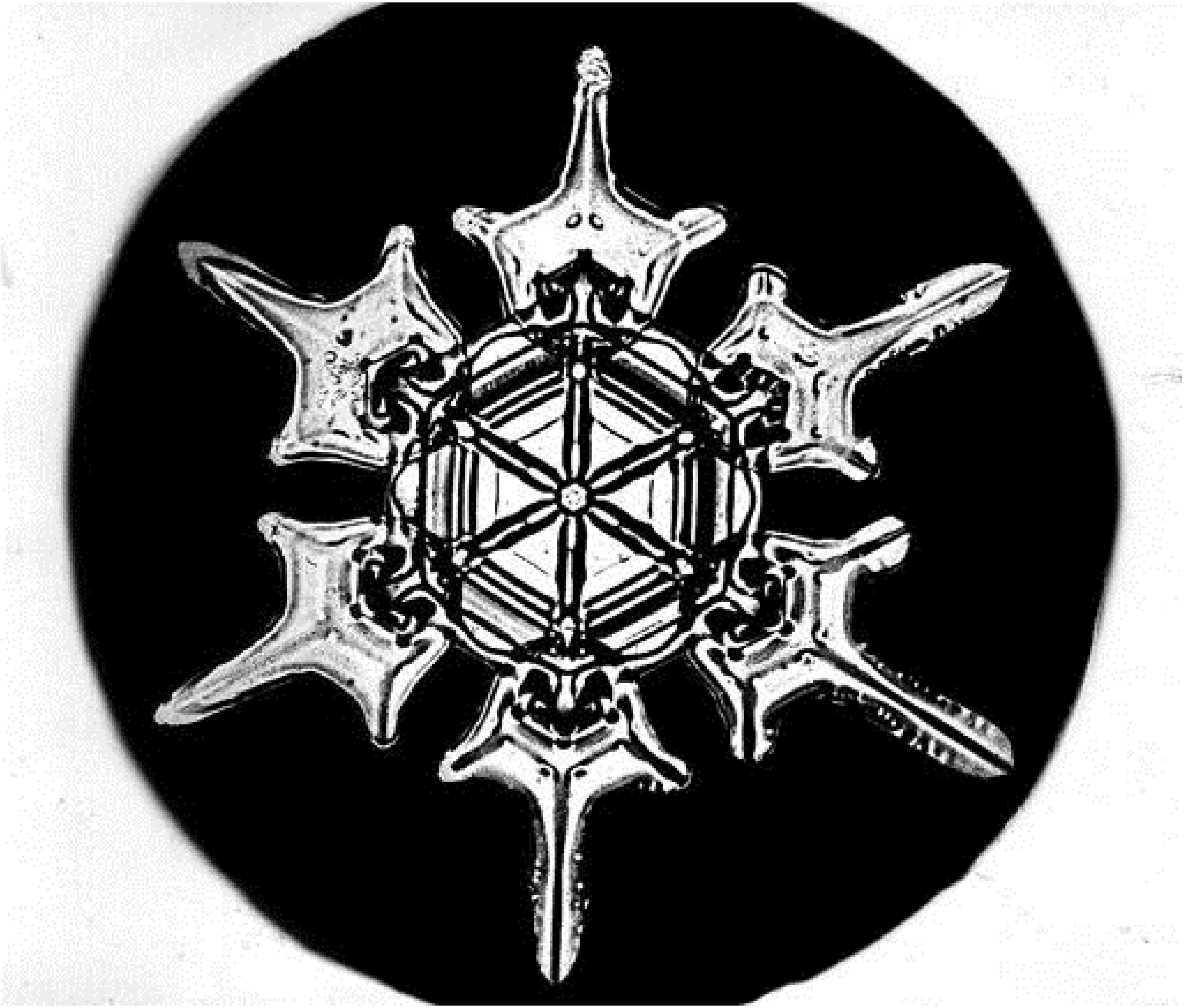
Devices on MDM

- feature phones
- some smartphones w/o security settings

- unofficial channels used to purchase
- some BYOD

unknown devices

- jail-broken/rooted
- BYOD
- deliberately unmanaged?



Top 15 tips guide

- we published a Mobile Devices: Tips for Security & Privacy document and released it the same day as our report
- a collaboration with the Officer of the Information and Privacy Commissioner's office (OIPC).
- designed to be used by everyone – work or personal, BC or anywhere else
- 10 security-related tips, 5 privacy-related; all in (correct) priority order ☺

Summary of Mobile Devices: Tips for Security & Privacy

1. Password protect your device
2. Lock your screen
3. Encrypt it
4. Limit password attempts
5. Use anti-malware software
6. Don't jailbreak or root your device
7. Be choosy with apps
8. Limit app permissions
9. Keep software up-to-date
10. Limit location information
11. Review voice commands
12. Promptly report lost/stolen devices
13. Bluetooth, Wi-Fi, NFC
14. Safely dispose of your device
15. Consider using Find My Phone

marketing

Downloads

Report	560
Tips	248

Social media impressions*

LinkedIn

909 (lock your screen – #2)

Facebook

871 (password protect your device – #1)

Twitter

288 (use anti-malware – #5)

* from "Tips" promotion 2017-Jan

conclusion

- we feel we provided value (to auditee and citizens)
- collaboration with the OIPC was win/win
- gov't responded promptly to some findings (best day ever!)

questions?

John Bullock, BSc, CISSP, CISA, CRISC, GICSP
Senior IT Audit Specialist
Office of the Auditor General of BC
jbullock@bcauditor.com
+1 250 419 6214