iPads: Love'em, Hate'em, You're Going to Have to Deal With'em

Mark Nunnikhoven
@marknca

Courtesy of Apple

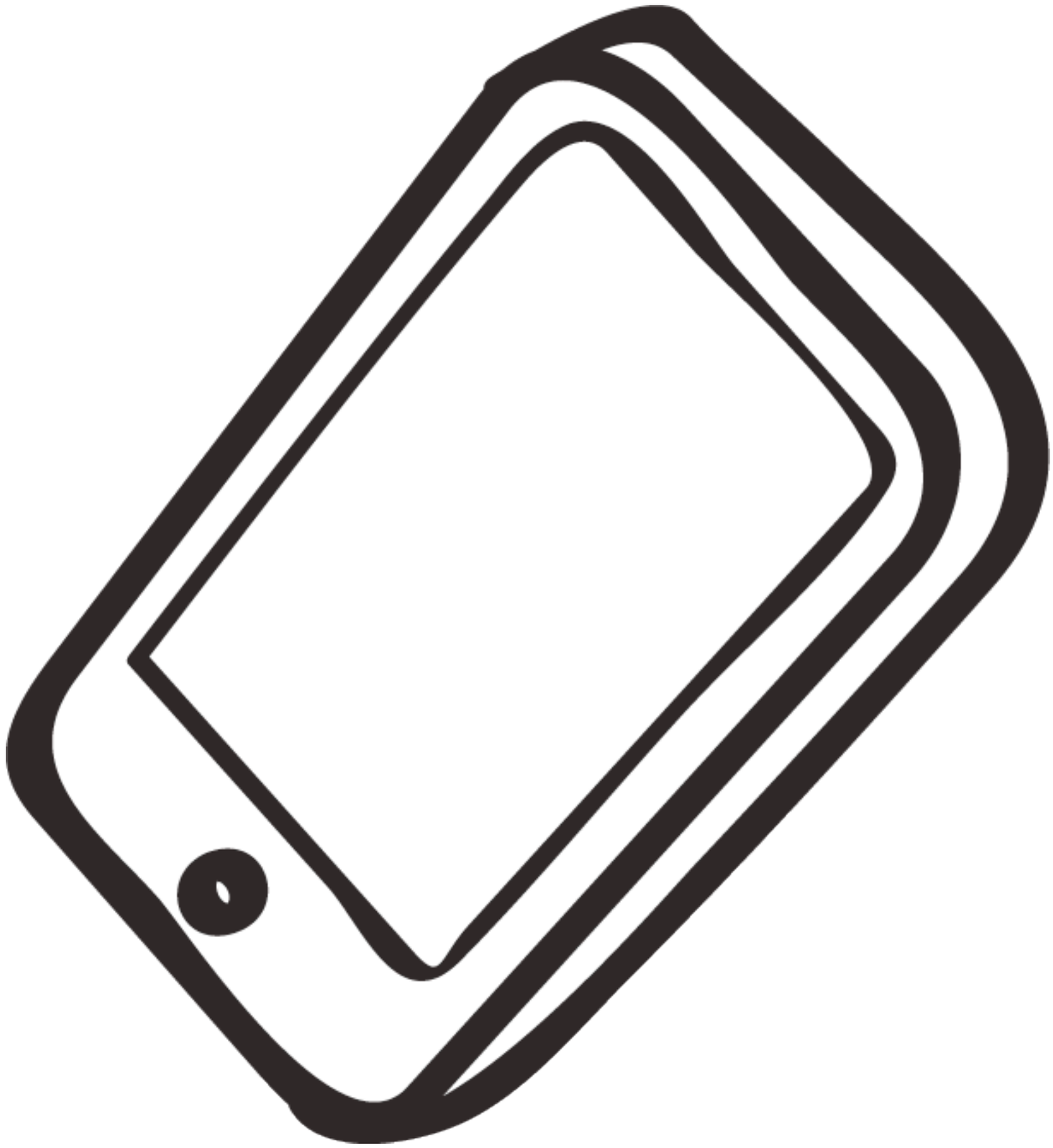
iPad2

Courtesy of Apple

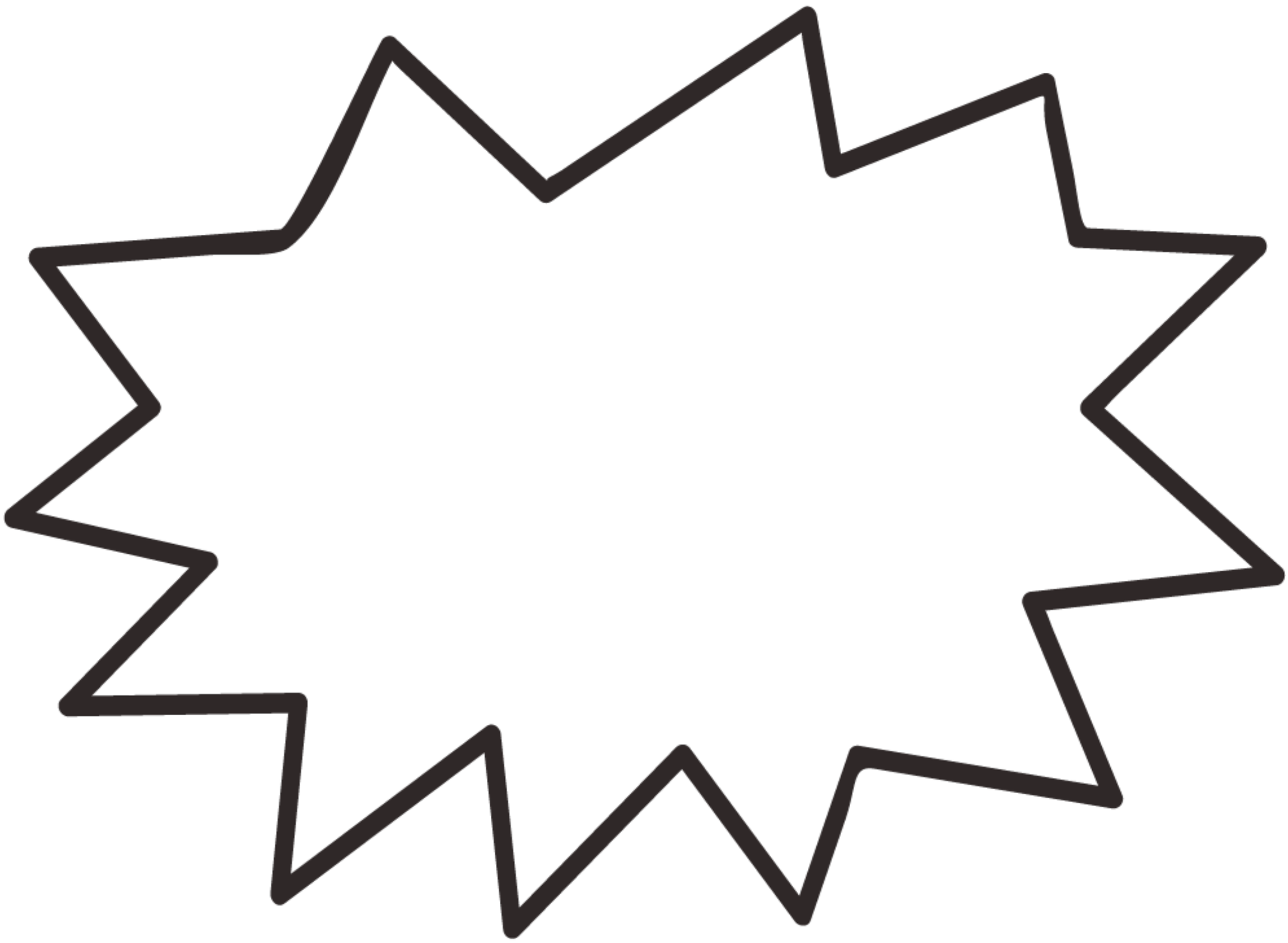
iPhone 4

Courtesy of Apple

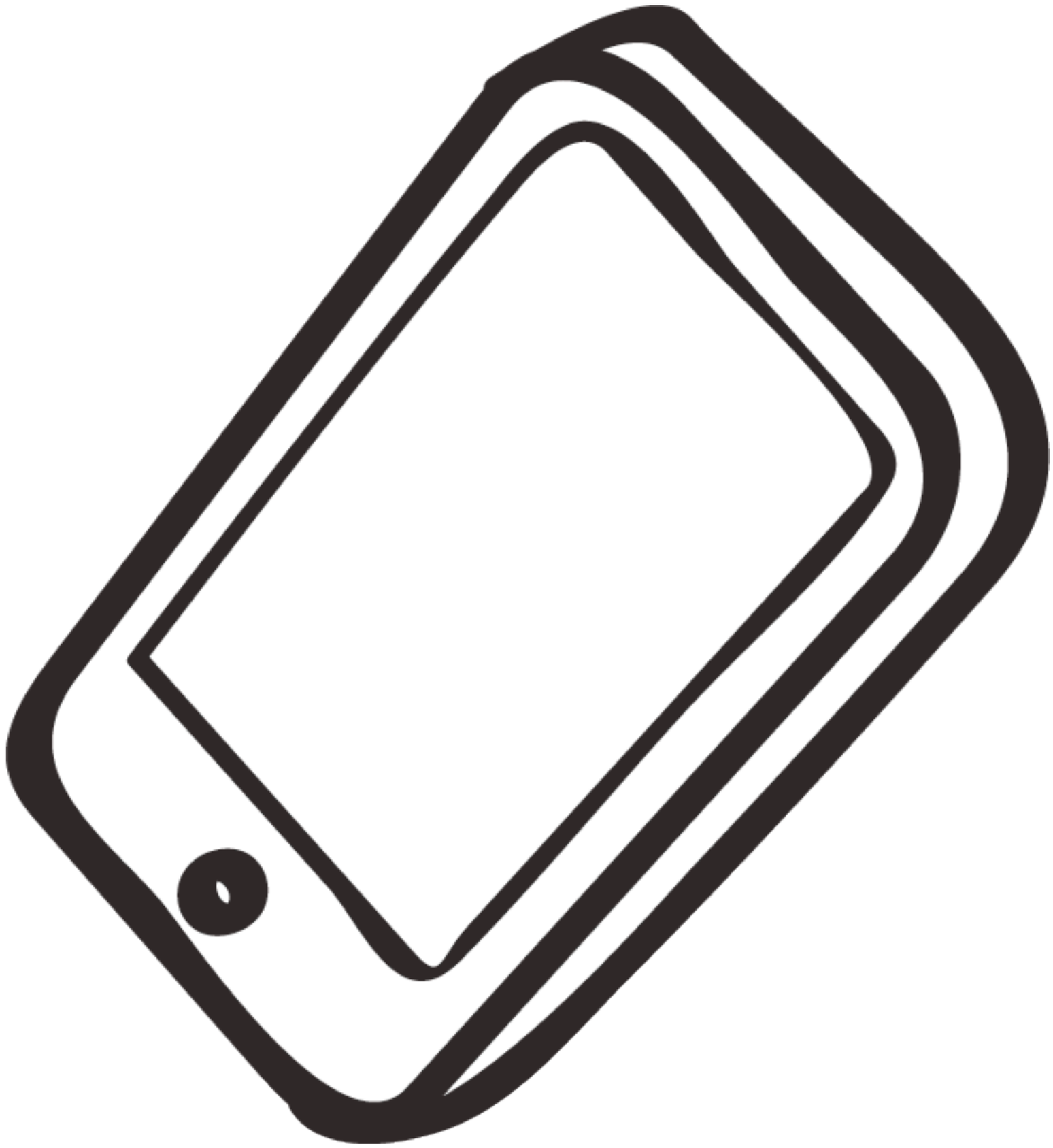
iPod Touch
- Guitar Hero
- Madden



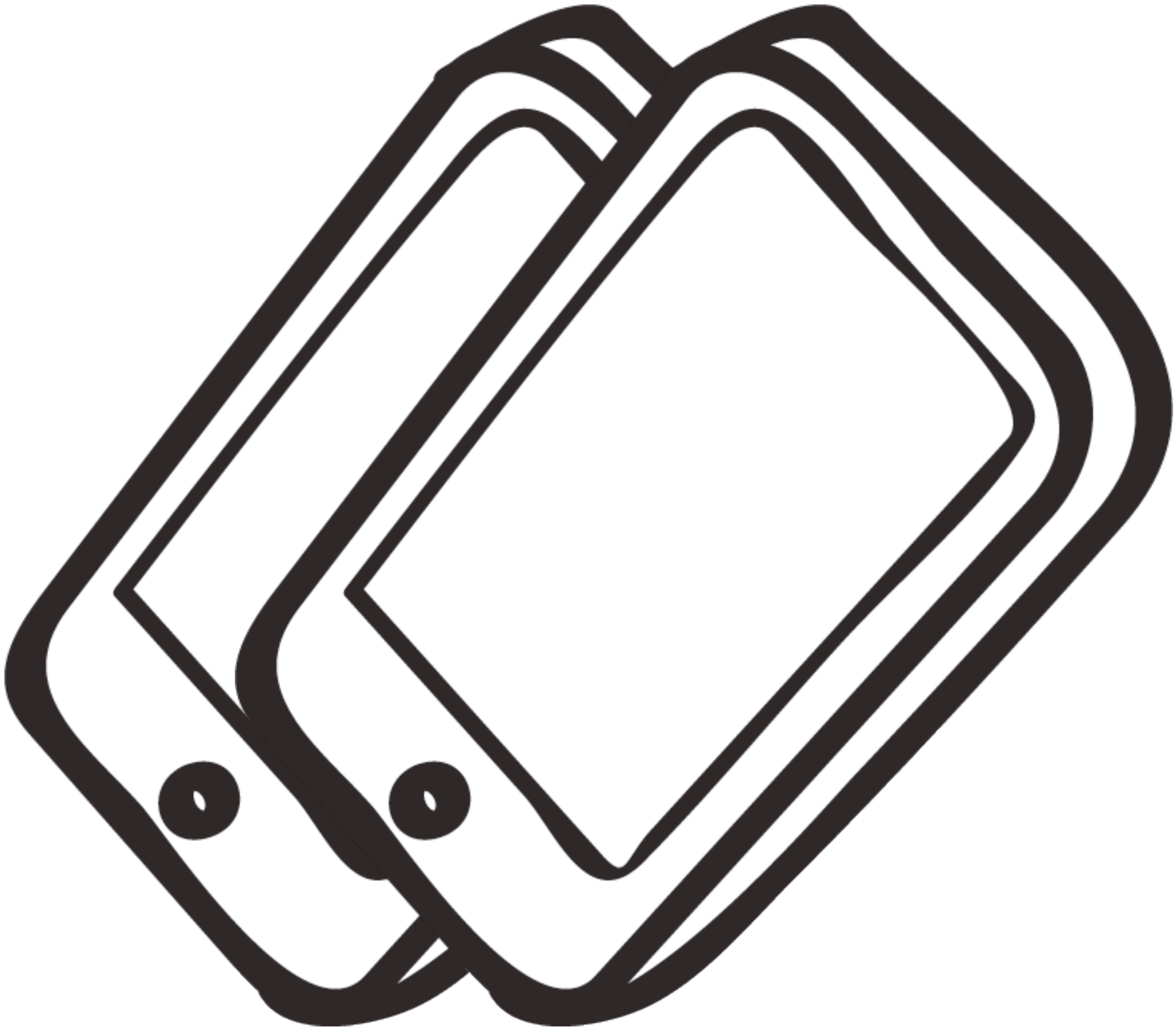
How do iPads show up in the enterprise?
- someone shows up to a meeting with one
- everyone oohs and ahhs



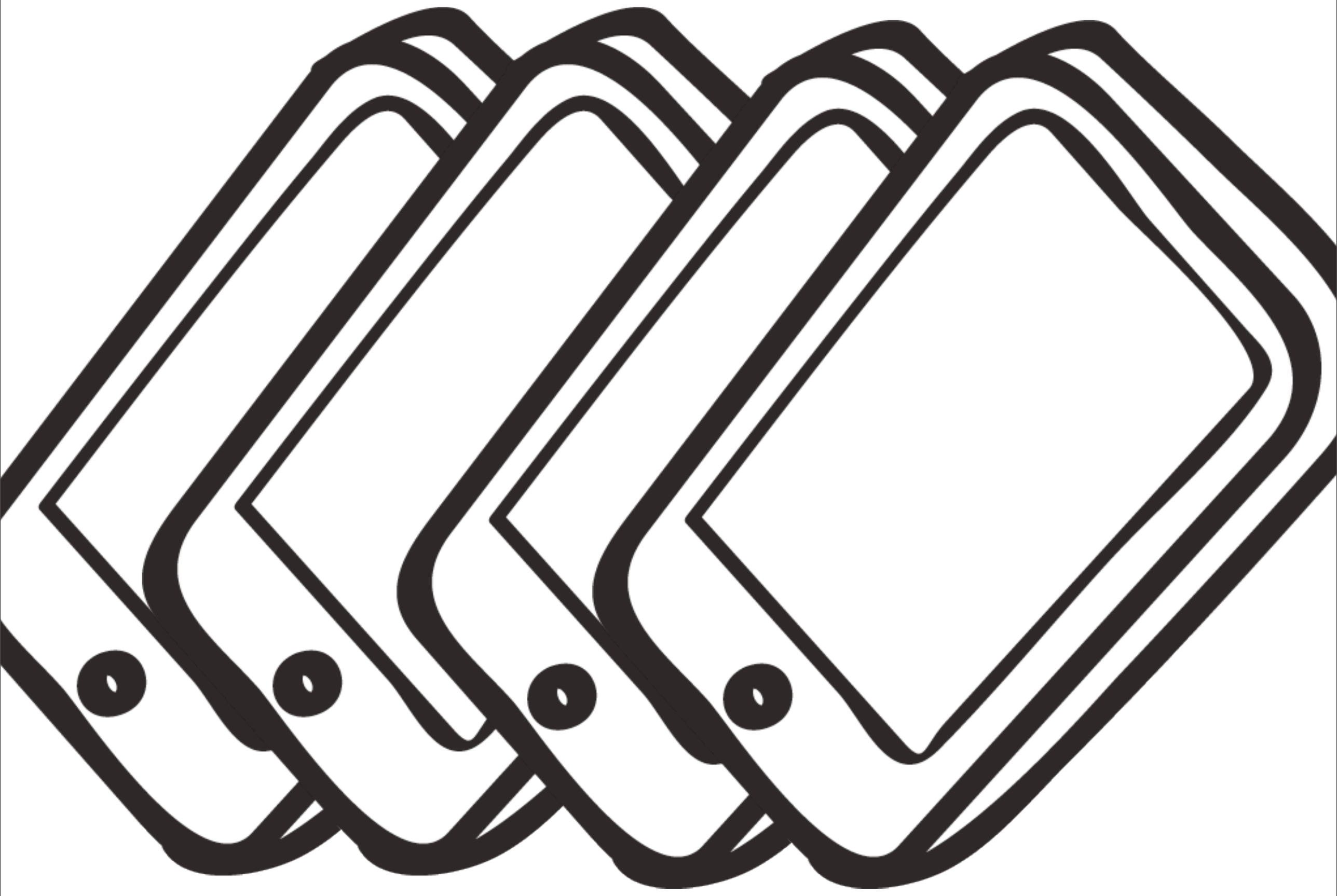
- ka-chow!



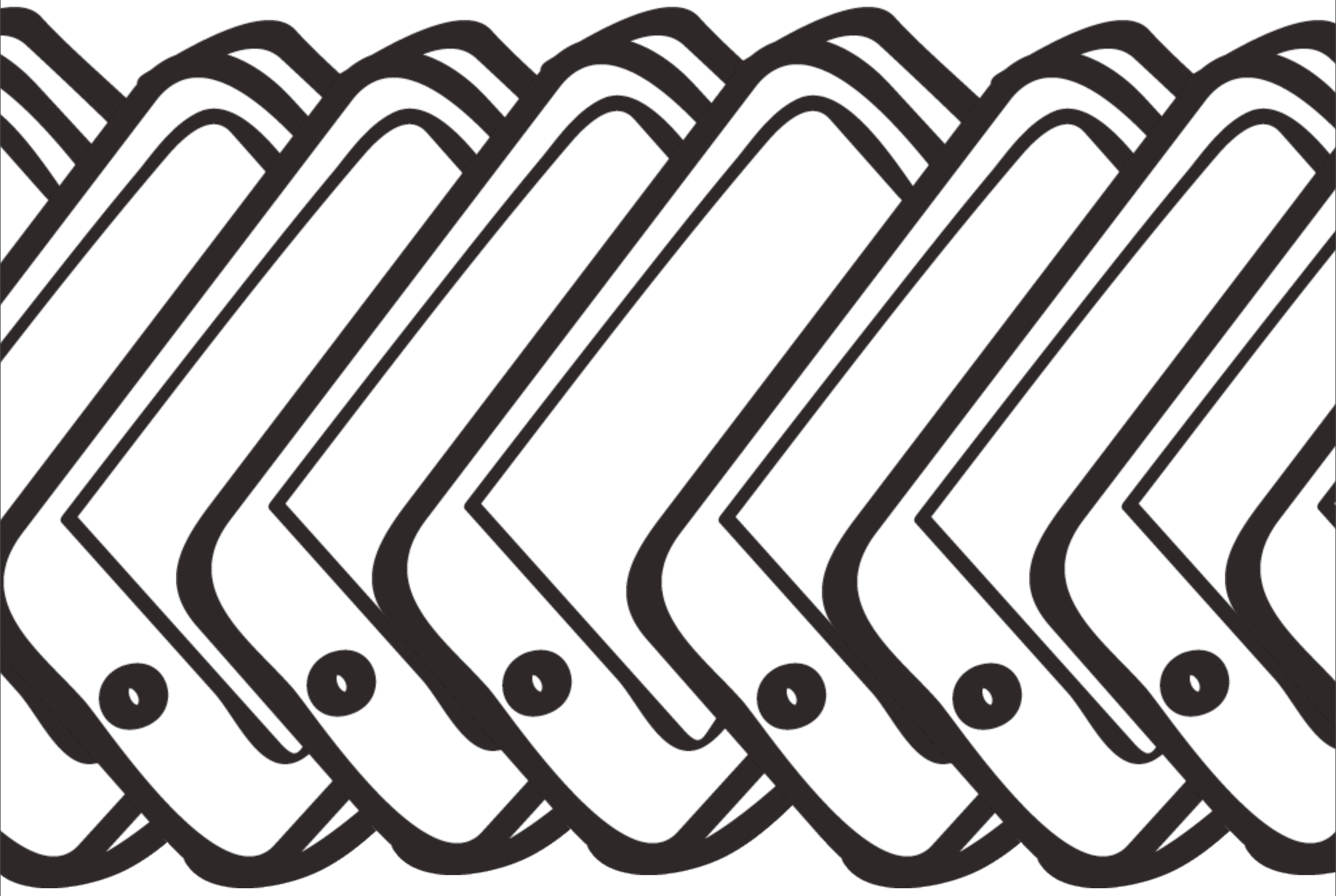
- one appears in the CEO’s hands



- then the CFO



- then the rest of the C-suite



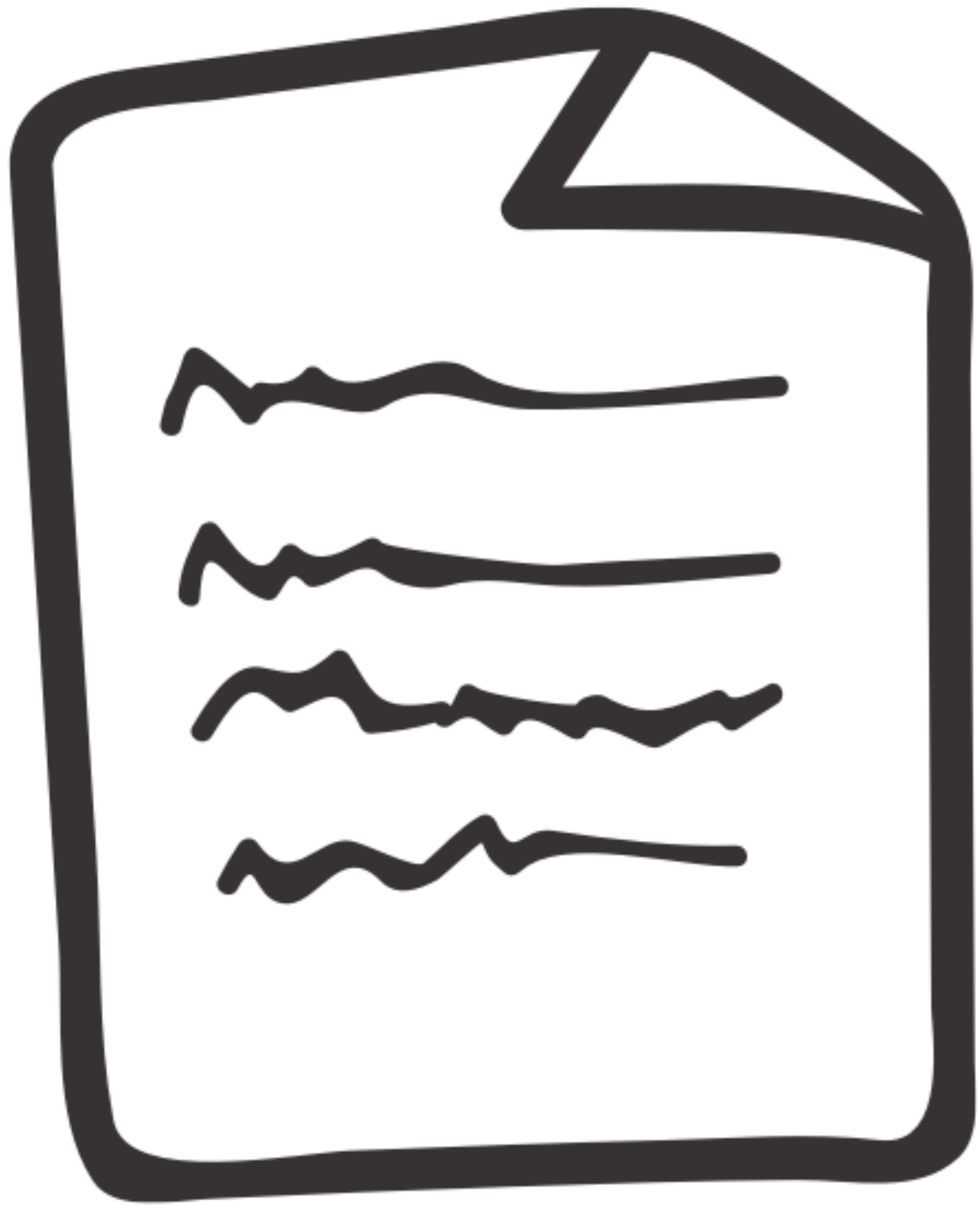
- then all of the executives jump on the bandwagon

Now what?

You're f$%ked

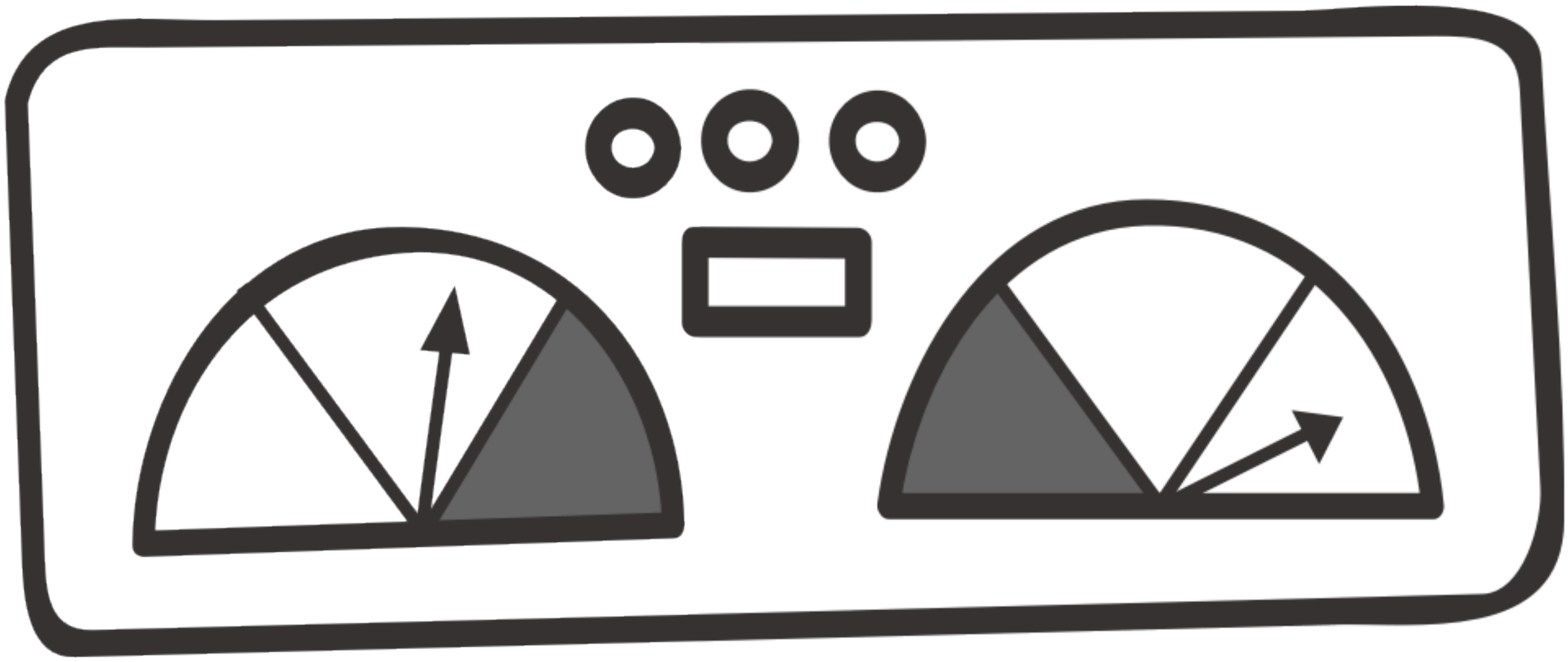
OK, so now what?

- grab a coffee

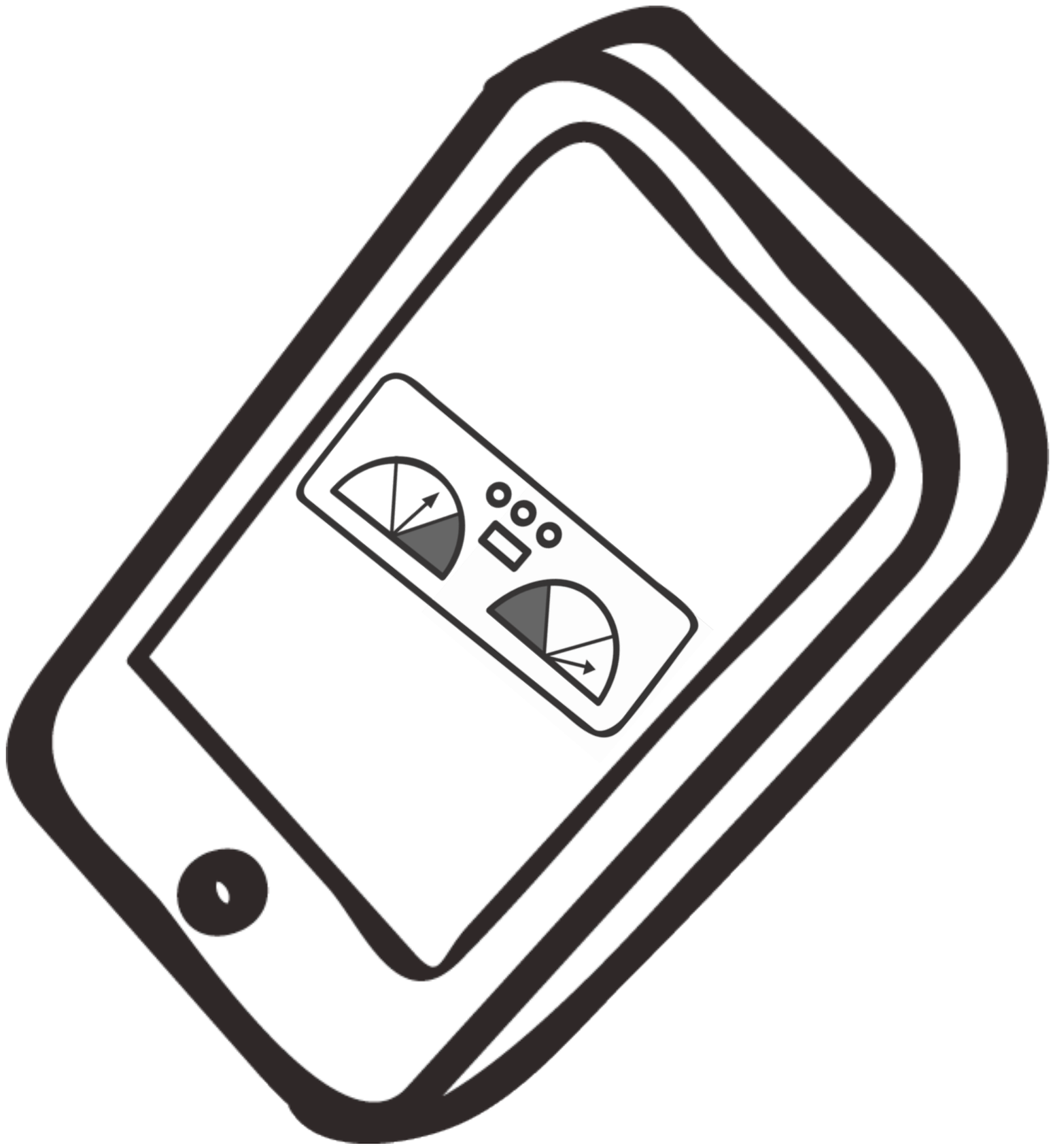


- gather some information about the risks and possible mitigations

- present the plan as a report to management
- that’ll get shot down



- add a dashboard somewhere in the project



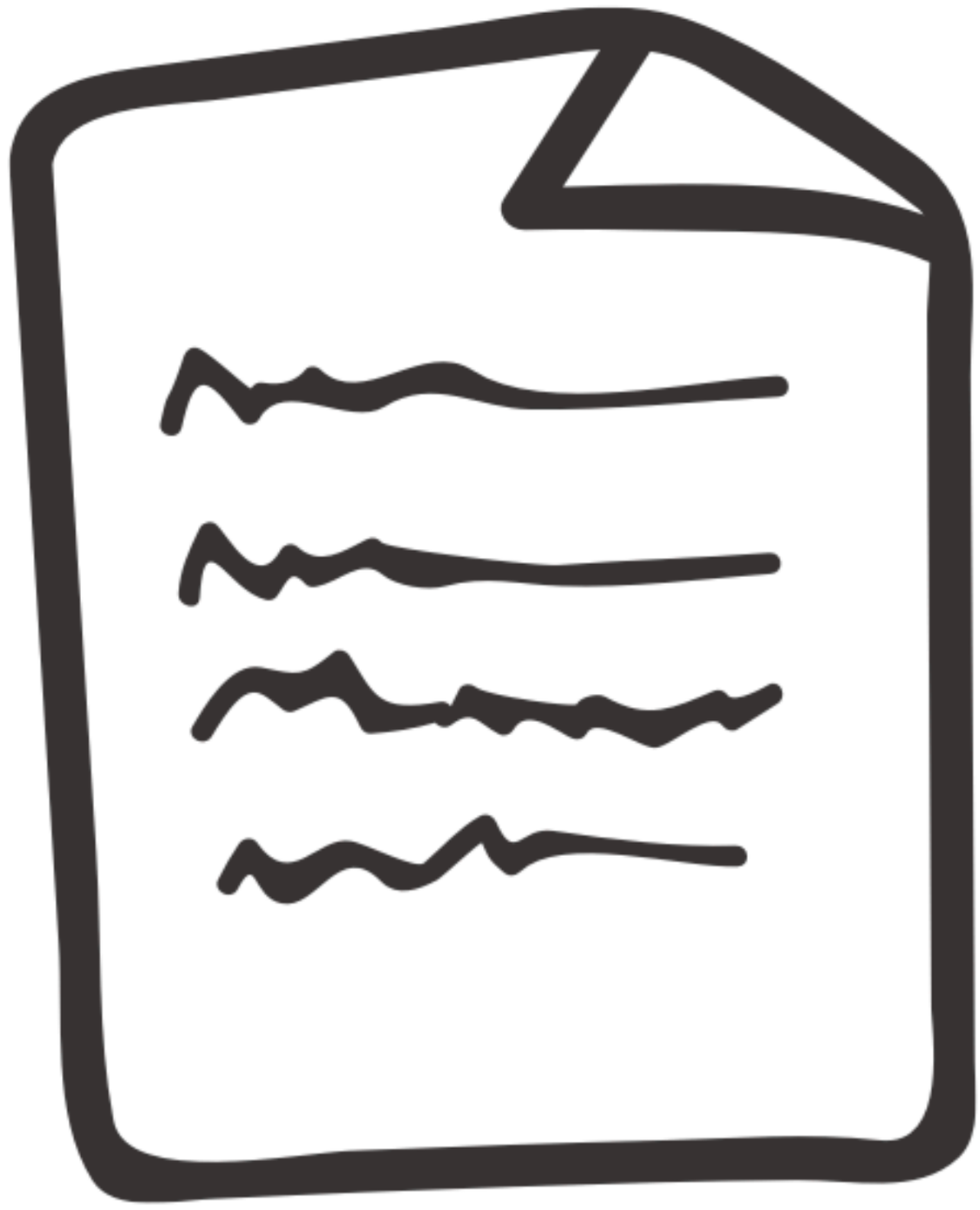
- better yet, tell them they can have the dashboard on their shiny new iPad

- present the plan as a report to management again
- get approval

Implement

- time to start putting controls in place
- bring all the current devices under central management
- maintain current and roll out more devices

Good news

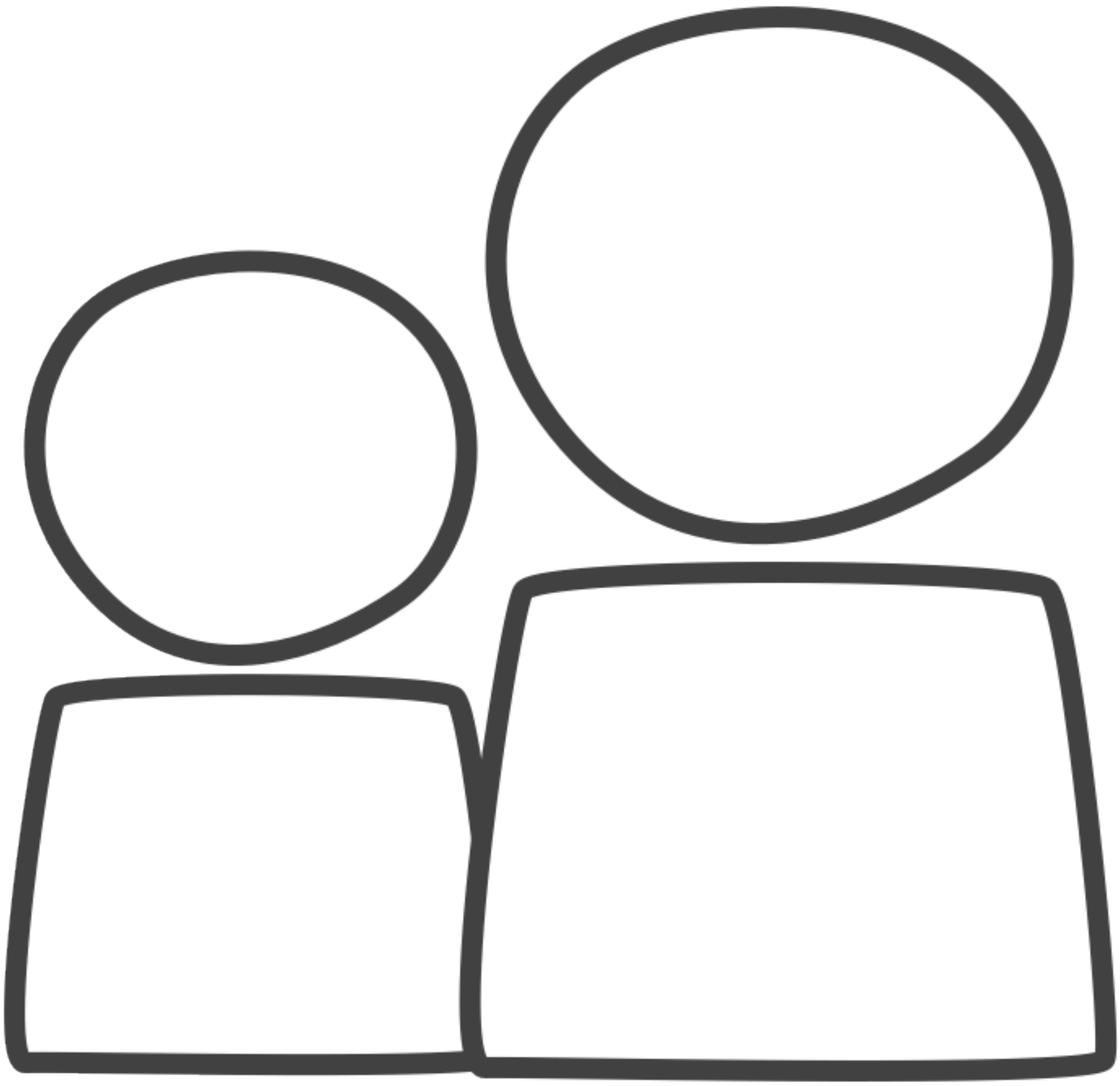


- I’ve already gathered a lot of the required information
- publishing it today/this weekend at http://markn.ca/2011/ios4
- feel free to slice & dice it, rework it
- all I ask is for attribution
- we will hit the high points today

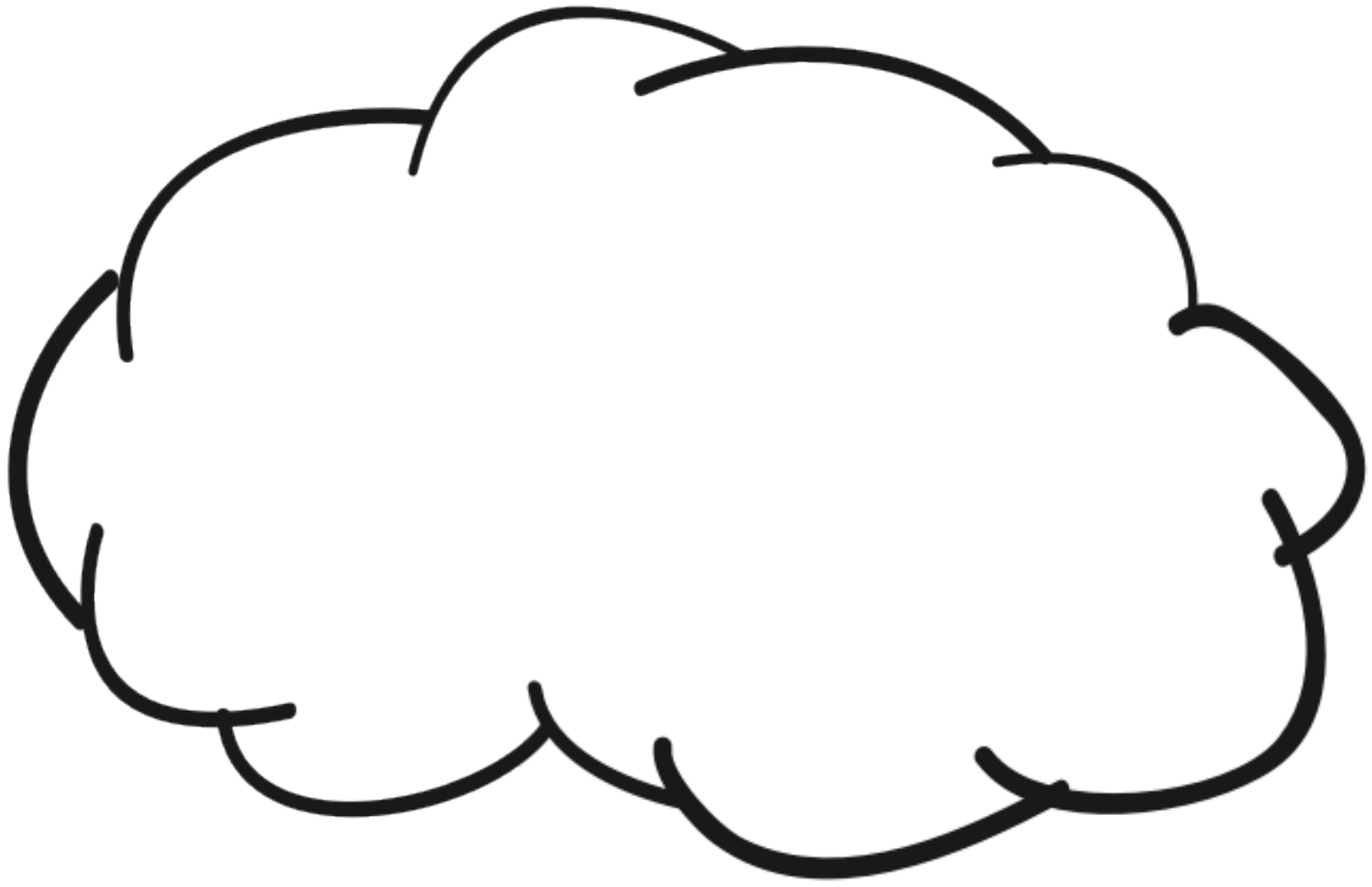
Let's get cracking

Remember

– things to keep in mind



- the user is king



- the ecosystem is very important
- enterprise services will be competing with the users expectation based on their cloud experiences
- Apple is focusing on the ecosystem and it’s evolving rapidly

- how do can iOS be attacked?
- image from Warhammer 40K, copyright GameWallpapers.com

Safari / WebKit

- typical browser
- apps are sand-boxed, DEP, ASLR = all helps isolate program execution
- exploits = mainly crashes, very few data leaks

Jailbreak!

- uses DFU mode to load crack iOS version
- allows for installation of unauthorized apps
- breaks sandbox assumptions
- DFU is how we restore & upgrade, also how we image forensically

Fraunhofer

- 6mins to keychain info
- lots plaintext in keychain that probably shouldn’t be
- design decision

ElcomSoft

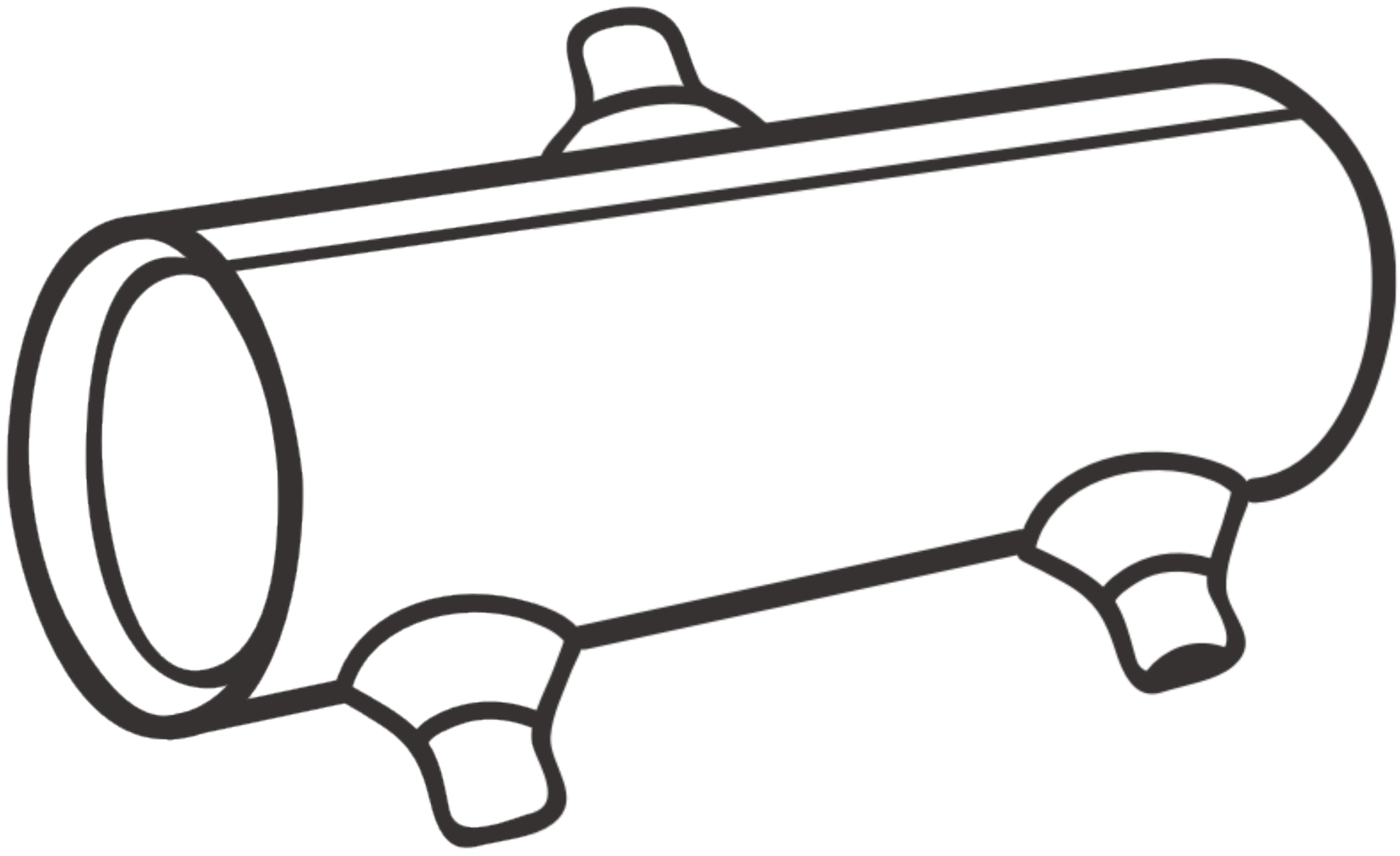
- bad passcode = easy to crack
- handy product
- bypasses brute-force sequence [1, 5, 15, 60, 60 min] on device
- lockout sequence goes exponential after 2nd 60 if you let it (have seen 120+ days!)
- can leverage escrow keys
- pulls UID key to crack passcode

Sogeti

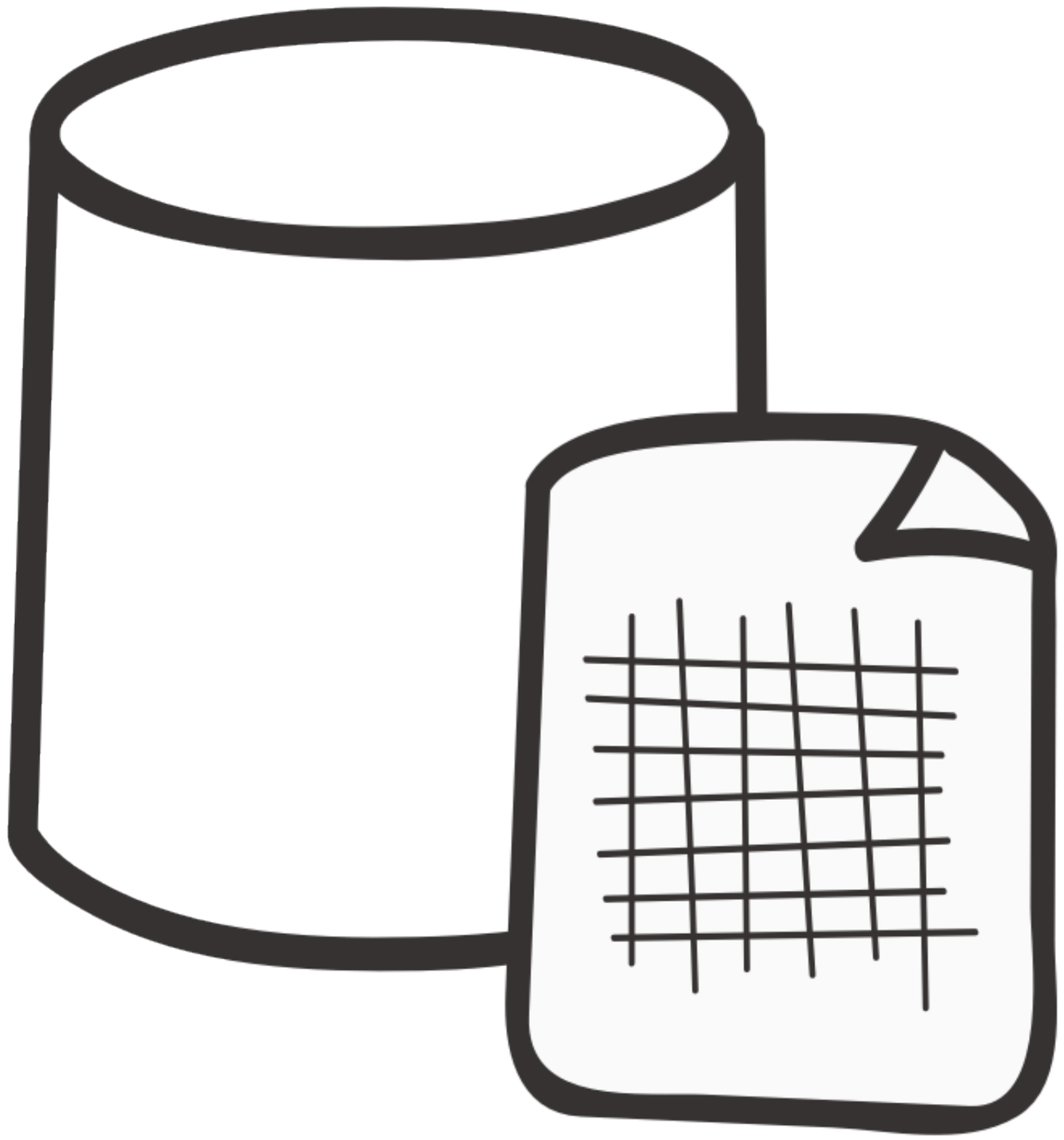
- provides deep dive into data protection framework
- released toolkit
- most of ElcomSoft product functionality available for free

Deployment

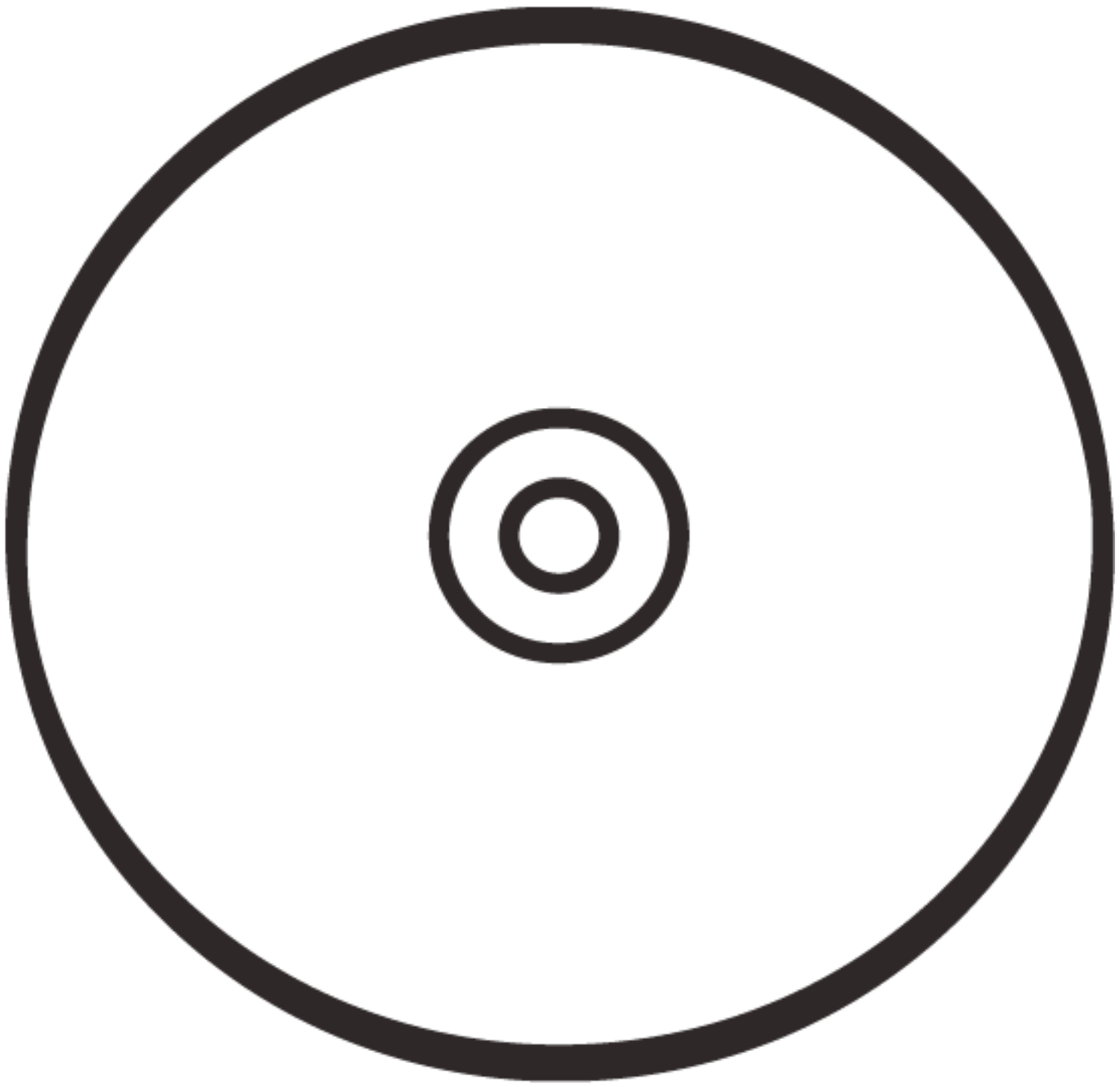
- next few slides will highlight the areas we need to address during deployment



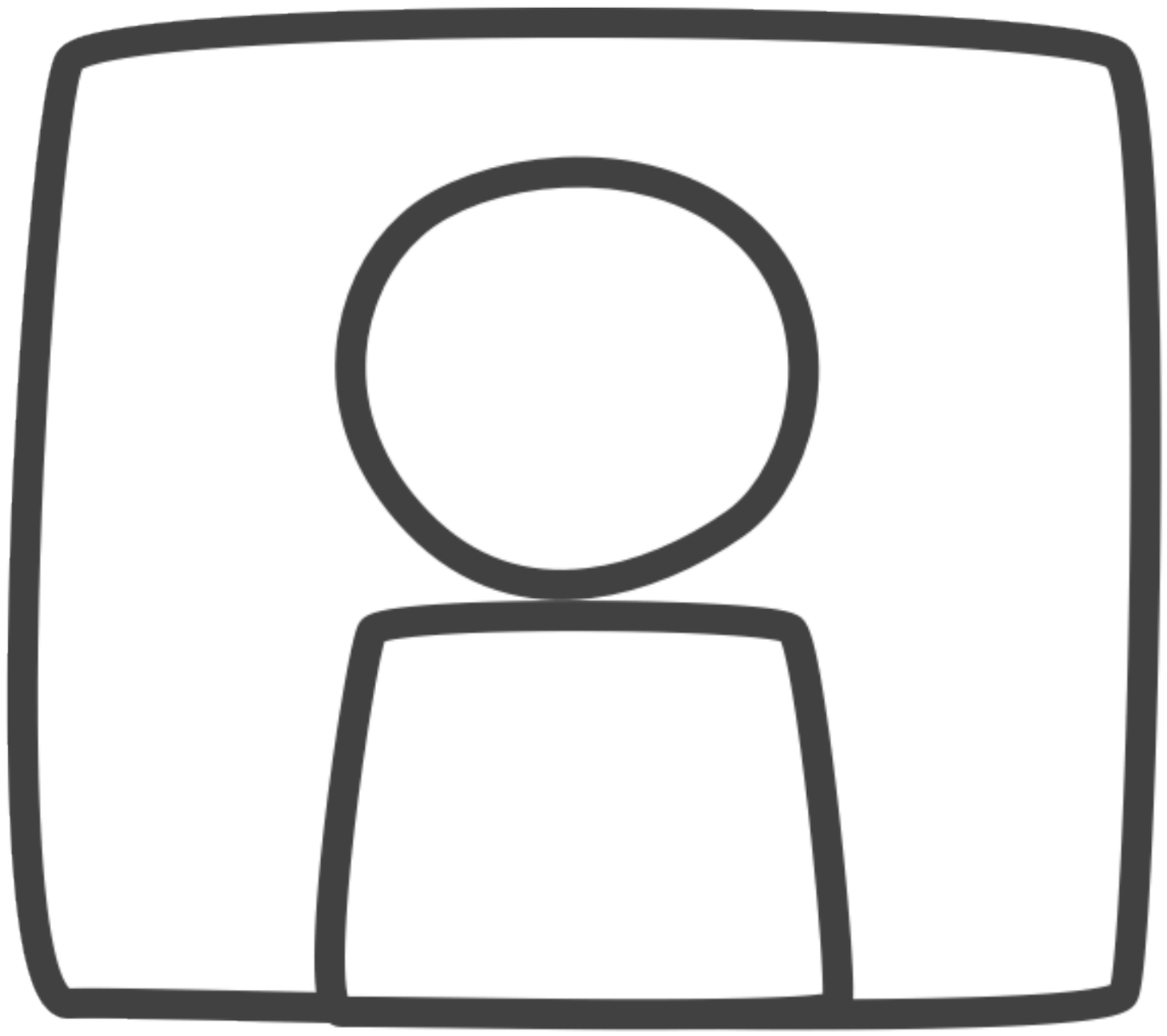
CONNECTIVITY
- 3G/wifi
- VPN
  -- Juniper, F5, Cisco == provide SSL support via apps
  -- on-demand is best
- personal hotspot
  -- prevents VPN bridging
  -- wifi/bluetooth/usb
- desktop/app virtualization
  -- official and unofficial clients
  -- how much of a footprint/forensic artefacts left on device after use?
- ActiveSync
  -- near-time delivery for mail/calendar/contacts == provides user's expected BB functionality
  -- allows for some policy & remote lock/wipe



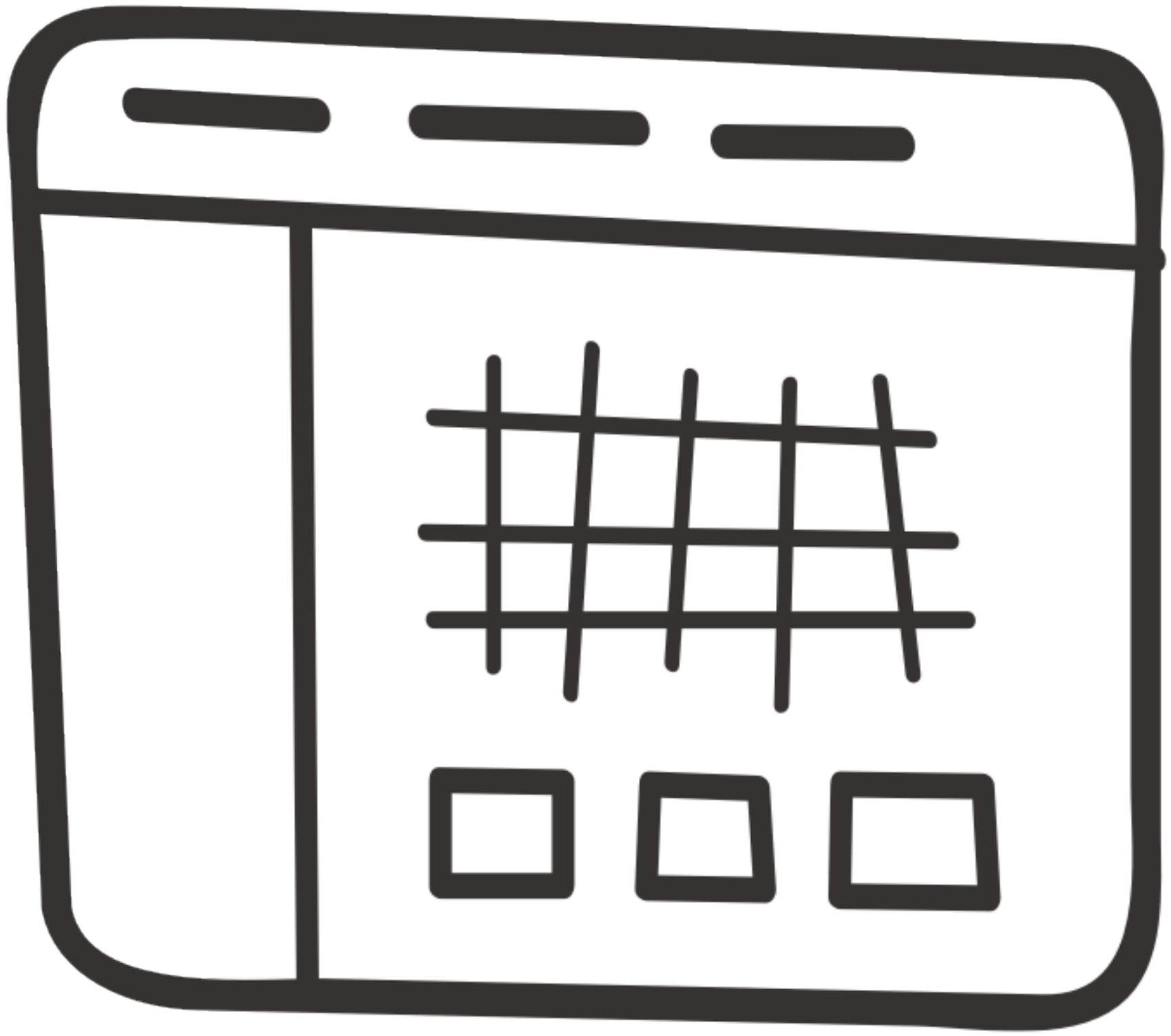
DATA AT REST
- data protection framework (DPF)
  -- whole device (well user partition) uses passcode + 50K rounds == key
  -- opt-in for file level
- document interchange
  -- makes 2nd copy of data
  -- expands risk to any new apps
- backups
  -- encrypt them, please!



iTUNES
- anchor around iOS' neck
- reduced role w/iOS 5
- maintenance
  -- contains WebKit
  -- can be configured (yes, even on Windows)
  -- auto-update tries to push other Apple products on Windows
- backups
  -- handles backups of iOS device
  -- handles backups of media/apps
- file transfer



MANAGEMENT
- profiles
  -- provides basic restrictions
  -- granular and aggro w/most restrictive winning
  -- usually provisioned via iTunes
- ActiveSync
  -- can enforce password policy
  -- adds remote wipe/lock
  -- remote locate via Apple or an MDM
- MDM
  -- automates the process
  -- some can manage other mobile devices (e.g., Android & BB's)
  -- if you have a lot of devices, it's worth looking into for provisioning alone



APPS
- in house or app store
- approving for the public store == pain in the @$$
- licensing a challenge for organizations

Recommendations

Read

- read the full set of docs for deployment that Apple provides

ActiveSync

- leverage ActiveSync from Exchange (most common) for password policy & remote wipe

On-demand VPN

- push all corporate & partner traffic---if not everything---through an on-demand VPN
- taking away user action == better security

MDM

- it’s just easier

Strong config profile

- start w/the template provided, mainly passcode length & complexity

Tailor iTunes

- it’s chatty
- media’s a pain
- f@%#ing WebKit

Ownership Policy

- make a decision on app and media ownership
- communicate it clearly

Educate

- conduct an education campaign about target for theft, etc.

Restrict Data

- don’t let key corporate data be stored on these devices
- good luck w/that!

Recommend Apps

- provide guidance for your user community

Review

- regularly review the whole deployment strategy
- make sure you’re always implemented the best plan for your org

Thank you

Mark Nunnikhoven
http://markn.ca
@marknca