Cyber Security and Data Management

THE EVOLVING LAW AND PRACTICE ON DELETING LARGE VOLUMES OF OLD DATA TO REDUCE CYBER RISK

Presented by
Avi Gesser, Davis Polk Litigation Partner
Gabriel Rosenberg, Davis Polk Financial Institutions Group Partner
Matthew Kelly, Davis Polk Litigation Associate

October 11, 2017

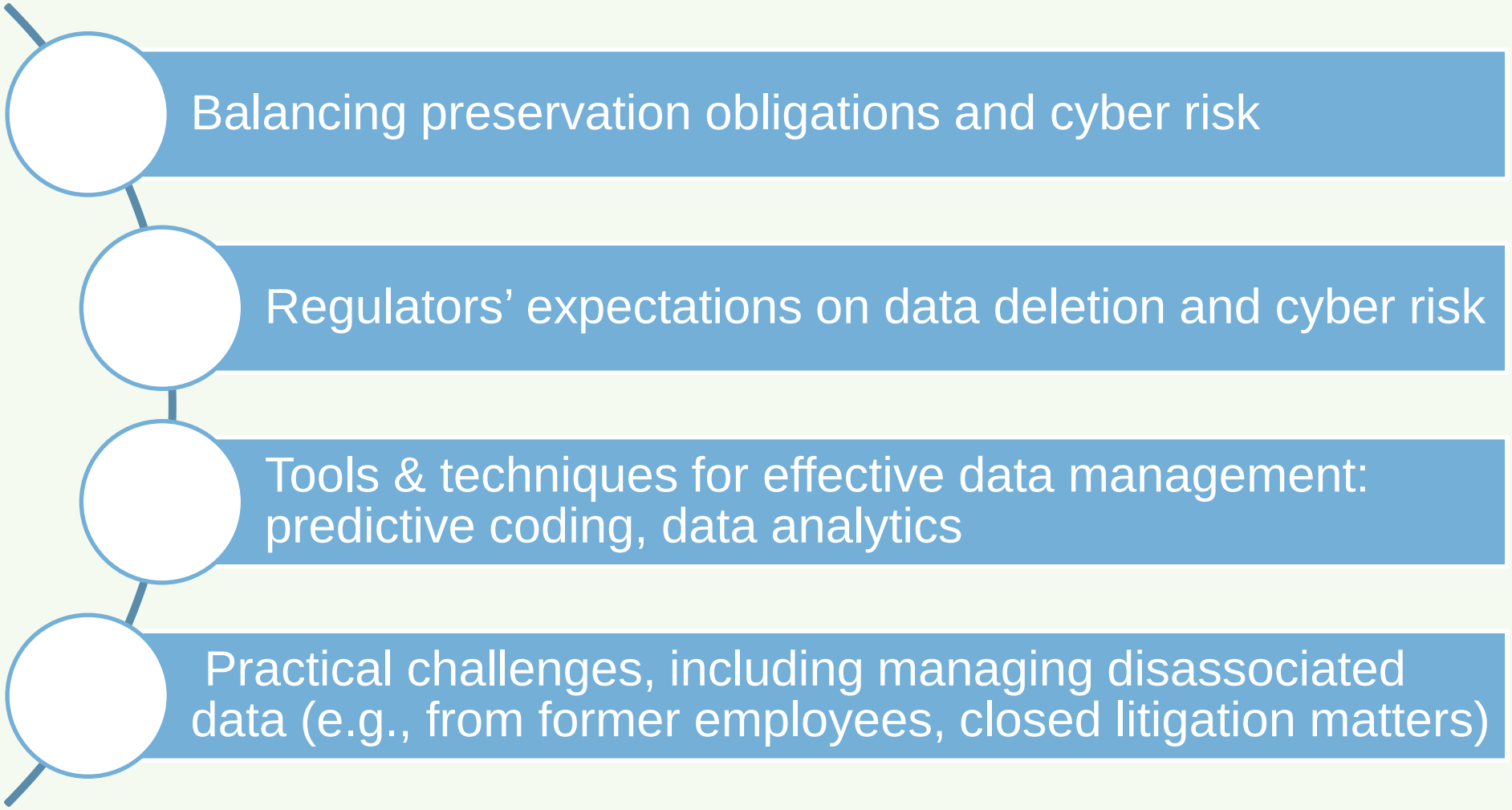
Davis Polk

Davis Polk & Wardwell LLP

CLE CREDIT AVAILABLE

WWW.CYBERBREACHCENTER.COM

Topics Overview



Data Management Is Essential For Effective Cybersecurity

How are data management and cybersecurity connected?

- Cybersecurity is about the protection of sensitive information from bad actors
- Growth in volume of data means more data that is at risk
- Variety of storage locations provides more opportunities for cyberattacks

How Did We Get Here?

Pre-Crisis Caselaw

- Developed in ad-hoc, case-by-case manner.
- Decisions arose only where something had already gone wrong.
- Difficulty in deciding what to keep leads to extreme bias against deletion.

Post-Crisis Litigation

- Entire industries subject to suit or investigation.
- Many retention policies (such as they were) suspended.
- Complex cases with long timelines prevent re-introduction of policies.

Big Data

- Data storage gets cheaper; indexing/analysis tools more widely available.
- Enthusiasm for “Big Data” initiatives drives active accretion of data.
- Overall culture shift in favor of data retention.

Keeping Everything is No Longer Viable

- It’s expensive
- It’s tricky to protect
- It’s unsearchable
- It’s unhelpful for litigation

Changes to the Federal Rules on Electronic Discovery

Advisory Committee Notes to FRCP Rule 37(e) read:

- *"The existing rule has not adequately addressed the serious problems resulting from the continued exponential growth in the volume of [ESI]. Federal circuits have established significantly different standards for imposing sanctions or curative measures on parties who fail to preserve electronically stored information. These developments have caused litigants to expend excessive effort and money on preservation in order to avoid the risk of severe sanctions if a court finds they did not do enough."*

Adverse inference sanctions only to be imposed where:

- A document existed and should have been preserved;
- The document was destroyed due to a party's failure to take reasonable steps to preserve it;
- The document cannot be restored or replaced through additional discovery; and
- The party that destroyed the document acted with intent to deprive another party of the information's use in the litigation

Changes to the Federal Rules on Electronic Discovery (cont.)

Hefter Impact Tech. v. Sport Maska Inc., 2017 WL 3317413 (D. Mass. Aug. 3, 2017)

- Defendant wiped laptop containing responsive documents after litigation-hold was in effect.
- Spoliation sanctions under 37(e) were not appropriate because documents were deleted as part of a companywide policy to wipe computers of employees taking maternity leave.
- No evidence defendant wiped employee laptop with intent to deprive plaintiff of evidence.

Changes to the Federal Rules on Electronic Discovery (cont.)

Martinez v. City of Chicago, 2016 WL 3538823, at *24
(N.D. Ill. June 29, 2016)

- Defendant not subject to spoliation sanctions for failure to preserve video evidence.
- No evidence of bad faith and court unwilling to infer bad faith based on speculation.
- Severe spoliation sanctions require more than negligence or gross negligence.

Changes to Regulations

NY DFS Regulation 23 NYCRR 500.13

- Obligates financial institutions to have:
  - *"policies and procedures for the secure disposal on a periodic basis of Nonpublic Information […] that is no longer necessary for business operations or for other legitimate business purposes of the Covered Entity, except where such information is otherwise required to be retained by law or regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained."*

Changes to Regulations (cont.)

FTC's Five Key Principles to Protect Personal Information

1. Take Stock – Know what personal information you have in your files and on your computers
2. Scale Down – Keep only what you need for your business
3. Lock It – Protect the information that you keep
4. Pitch It – Properly dispose of what you no longer need
5. Plan Ahead – Create a plan to respond to security incidents

Changes to Regulations (cont.)

Regulation EU 2016/679 (GDPR)

- Core Principles (Article 5):
  - Purpose limitation
  - Data minimization
  - Storage limitation
- Right to Erasure (Article 17):
  - Places obligation on companies to erase personal data without undue delay once requested
  - ECJ confirmed in 2014 the “right to be forgotten” (Google vs. Spain)

Why is it so hard to start?

- Starting the process requires:
  - Time and money
  - Clear ownership for the task (IT, legal, risk, compliance etc.?)
  - Handling diffuse and diverse data sources
  - Technical expert knowledge
  - Reliable technical solutions
  - Legal decisions throughout the process

Why Now is the Time to Start & How to Start

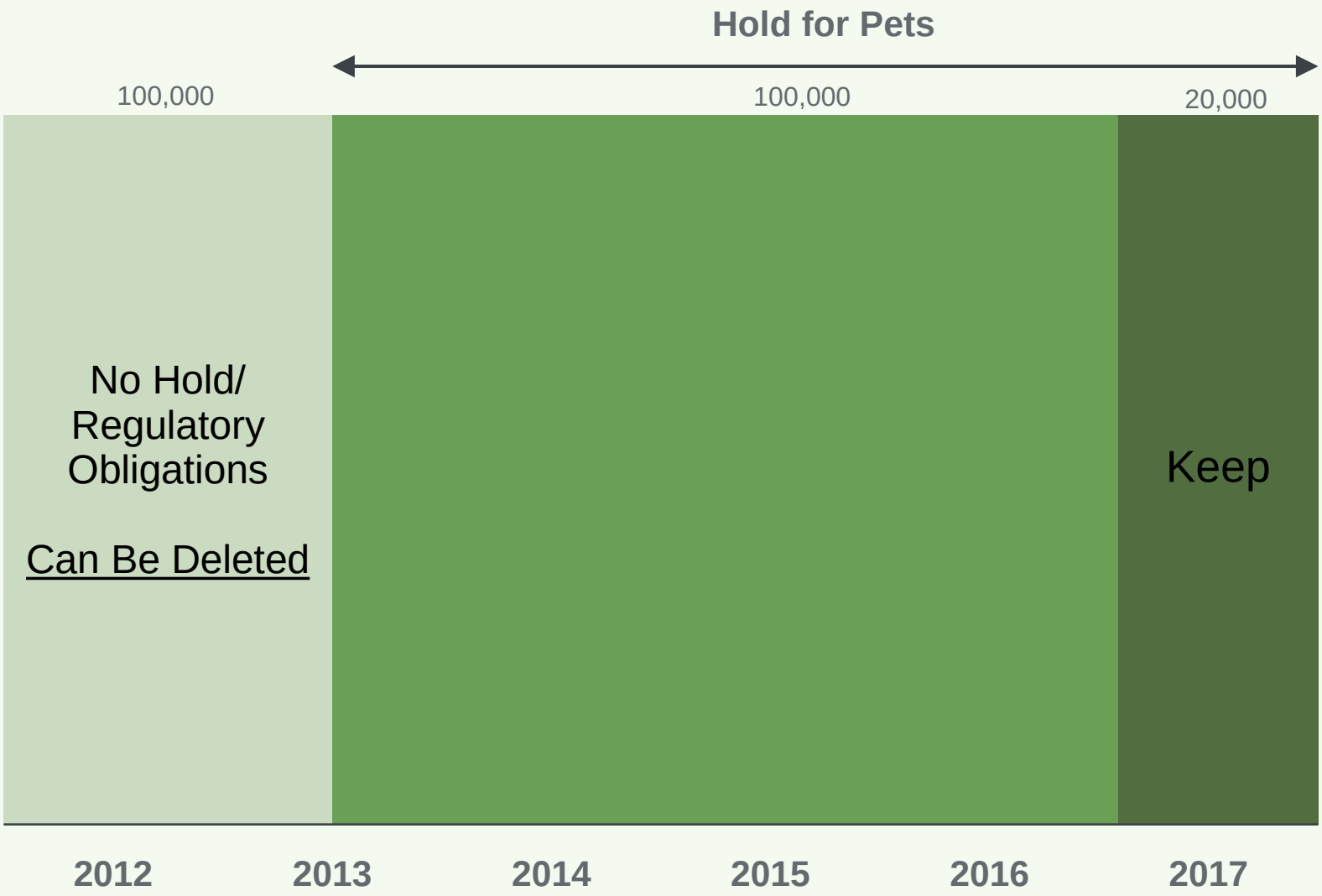
How do you start?

- Get system in place for new data
- Start small
- Start with oldest data

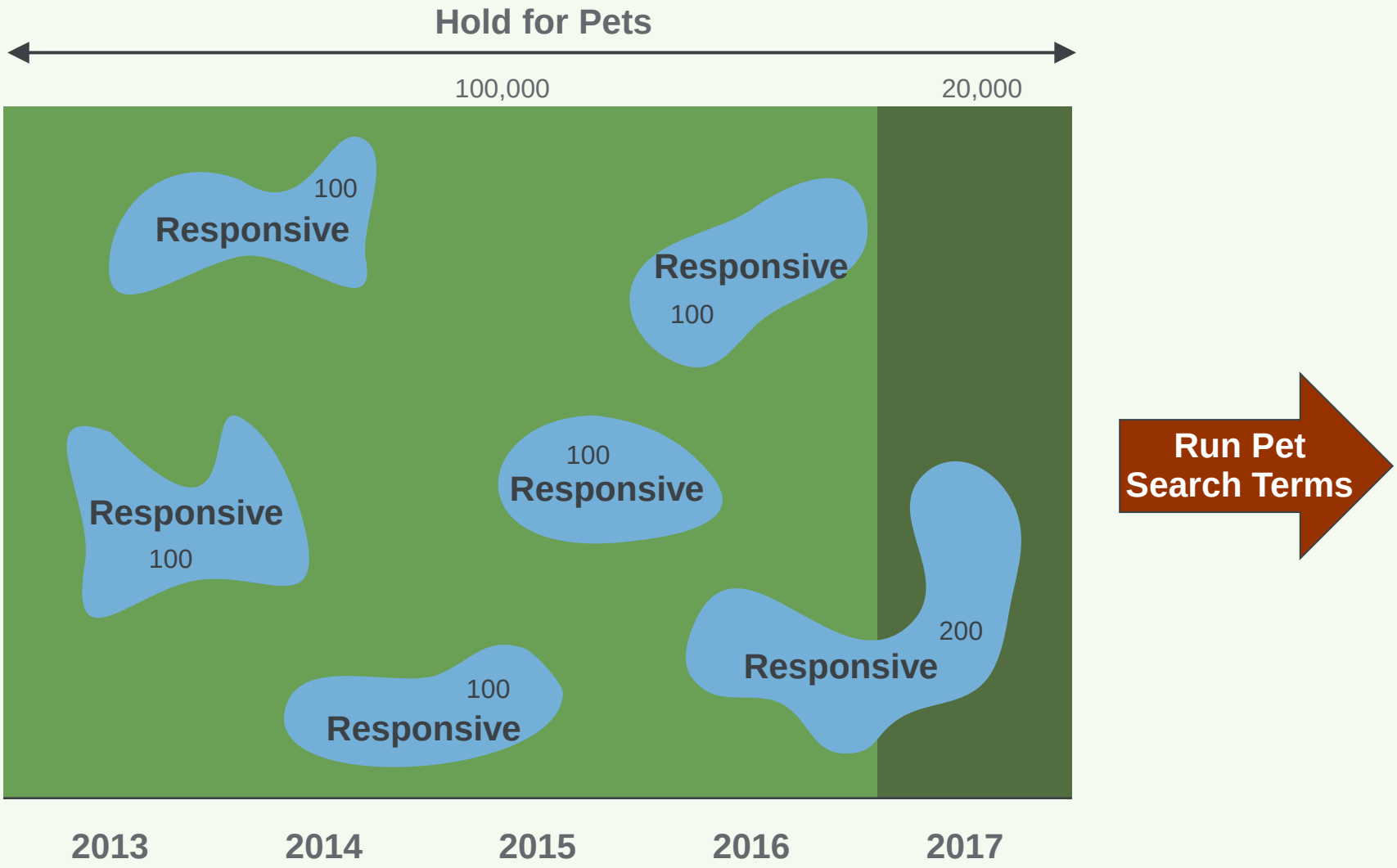
How do you start with recent data under holds and regulatory requirements?

- Search terms alone are too blunt
- Combine search terms and data analytics

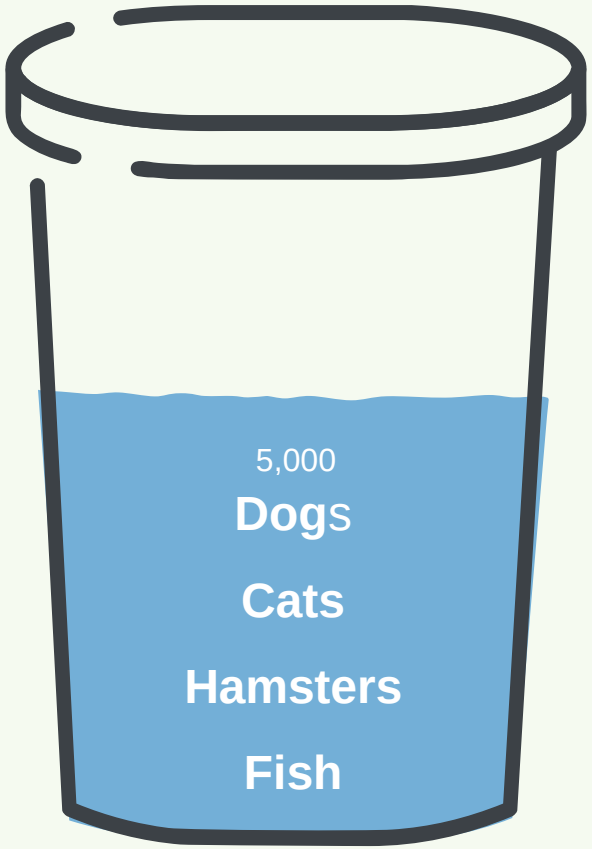
How to Start


Hold for Pets
100,000
100,000
20,000
No Hold/
Regulatory
Obligations
Can Be Deleted
Keep
2012
2013
2014
2015
2016
2017

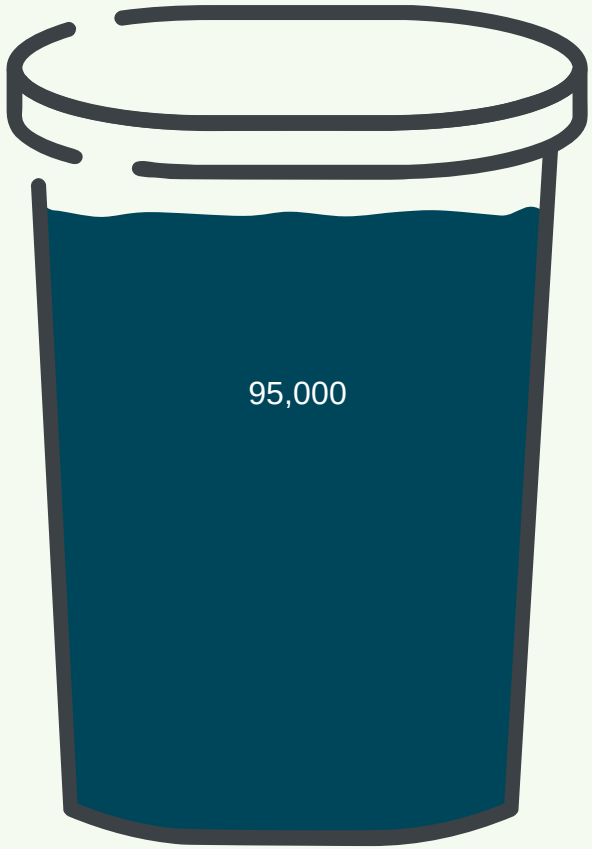
How to Start (cont.)



How to Start (cont.)

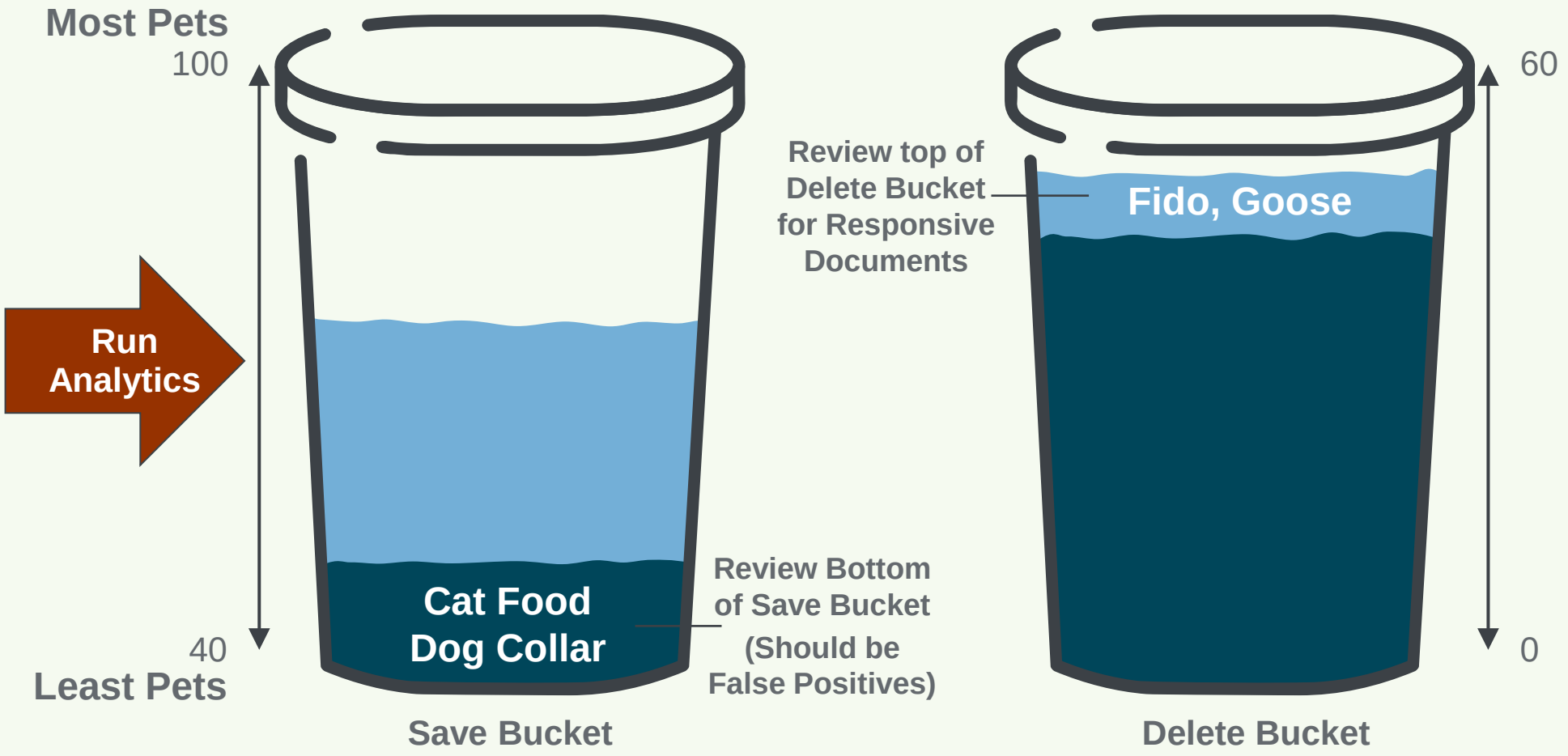


Save Bucket
Hit on Search Terms

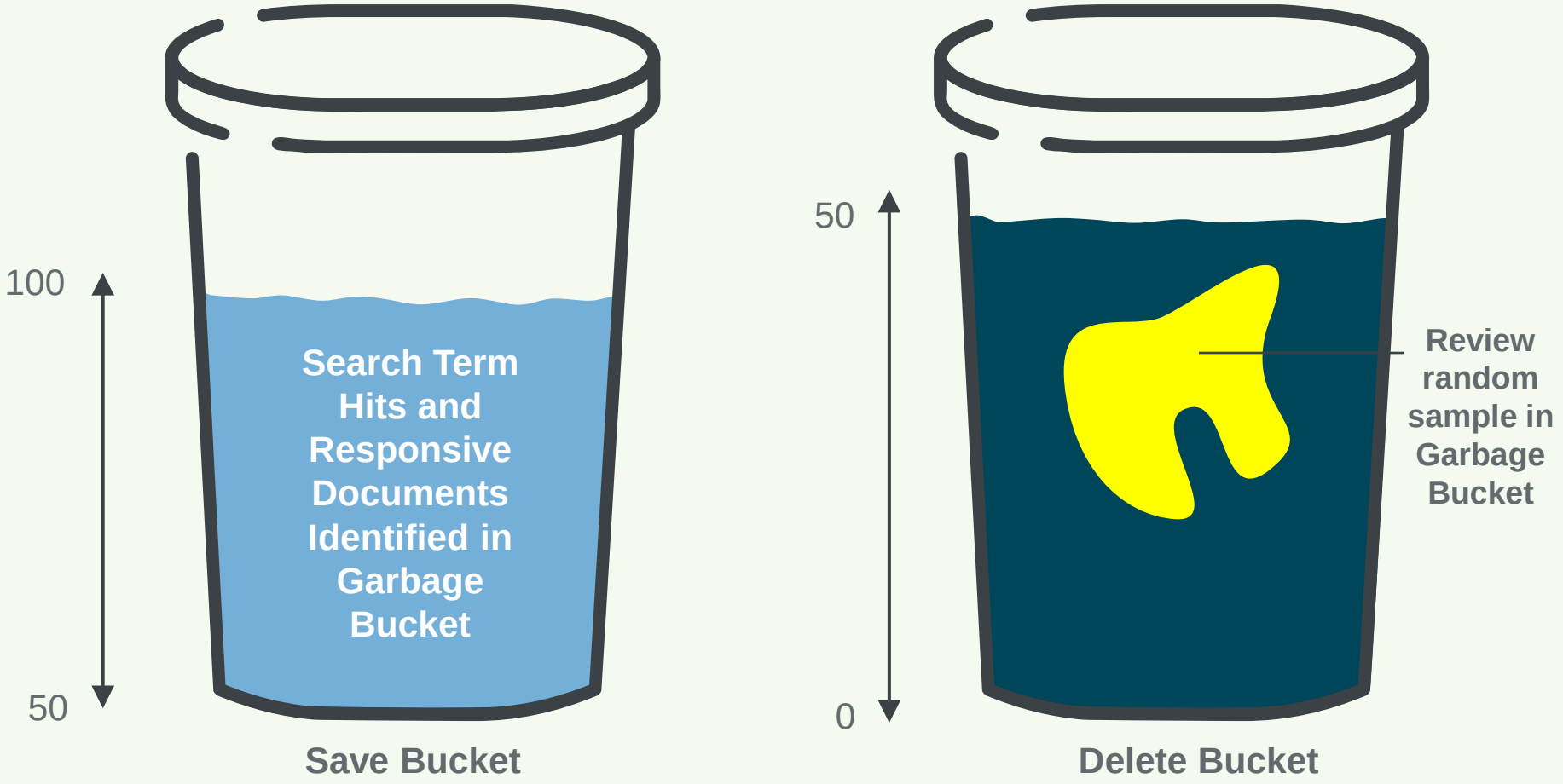


Delete Bucket
Did Not Hit on Search Terms

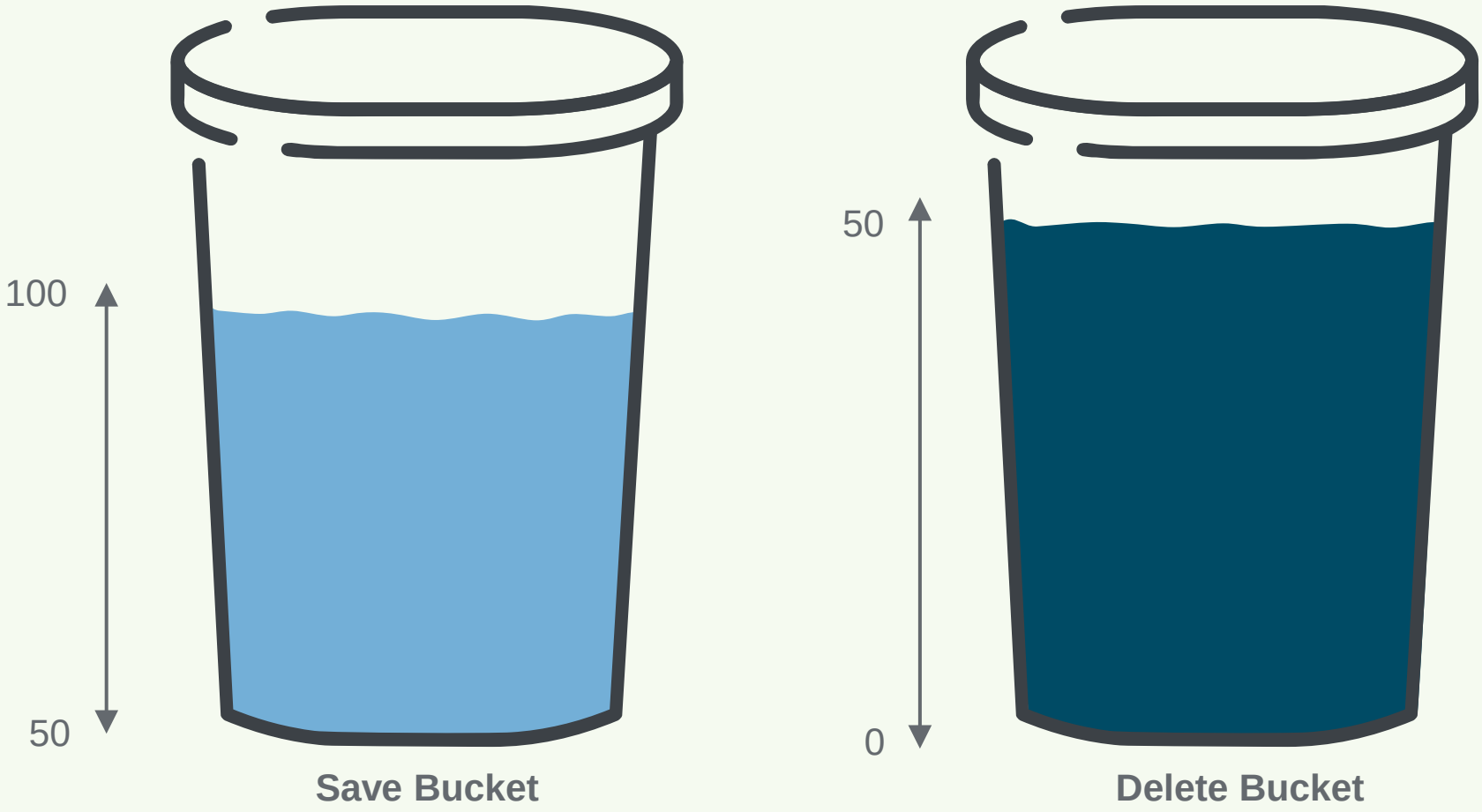
How to Start (cont.)



How to Start (cont.)



How to Start (cont.)



How to Start (cont.)

Complexities

- How do you handle custodians who are subject to multiple holds?
- How do you handle custodians who have multiple copies of the same emails?
- How can you group custodians together when doing this analysis?

How to Start (cont.)

Risks/Challenges

- How susceptible are the holds to analysis by the analytics?
- Are topics too nebulous to be captured by linguistic algorithms?
- How rich is the data?
- What if something that should have been preserved is deleted?

Combining search terms and data analytics using this protocol should mitigate most of these risks

Questions?

Visit: www.cyberbreachcenter.com