

ALISON GROUNDS – TROUTMAN SANDERS EMERGE

STEPHANIE MITCHELL – SIEMENS

SCOTT WANDSTRAT – ARNALL GOLDEN GREGORY

---

# ISSUES AND PRACTICES WITH DEVICES AND SOCIAL MEDIA

# OVERVIEW

---

- ▶ Facts and Figures – Statistics!
- ▶ Overview of the Legal Landscape
- ▶ Practical Strategies
  - ▶ Preservation
  - ▶ Collection
  - ▶ Production
- ▶ Overview of Authentication Issues





MOBILE DEVICE

---

# FACTS AND FIGURES

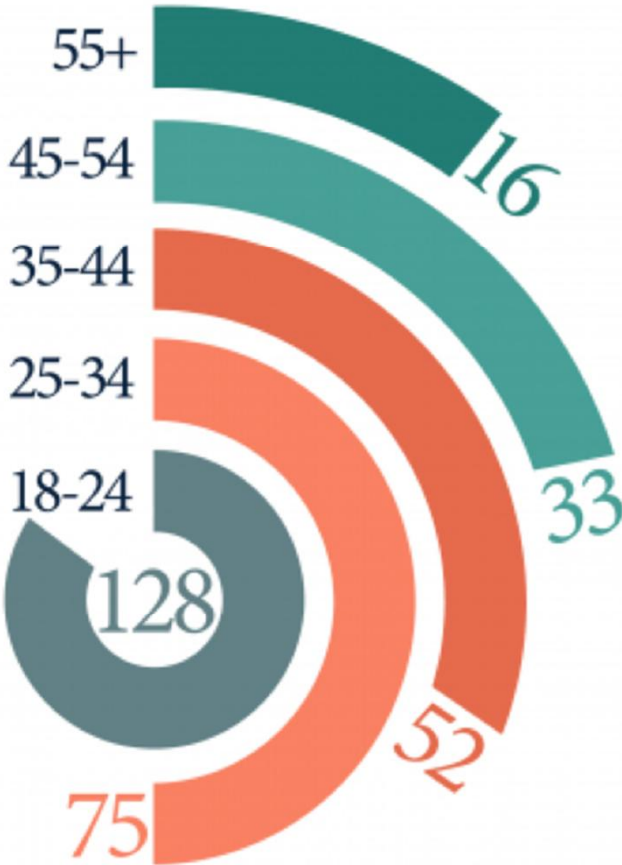
- ▶ 95% of American adults have a cell phone
- ▶ 77% of American adults have a smartphone
- ▶ 53% of American adults own a tablet computer

*Pew Internet Project Research 2018 Surveys*

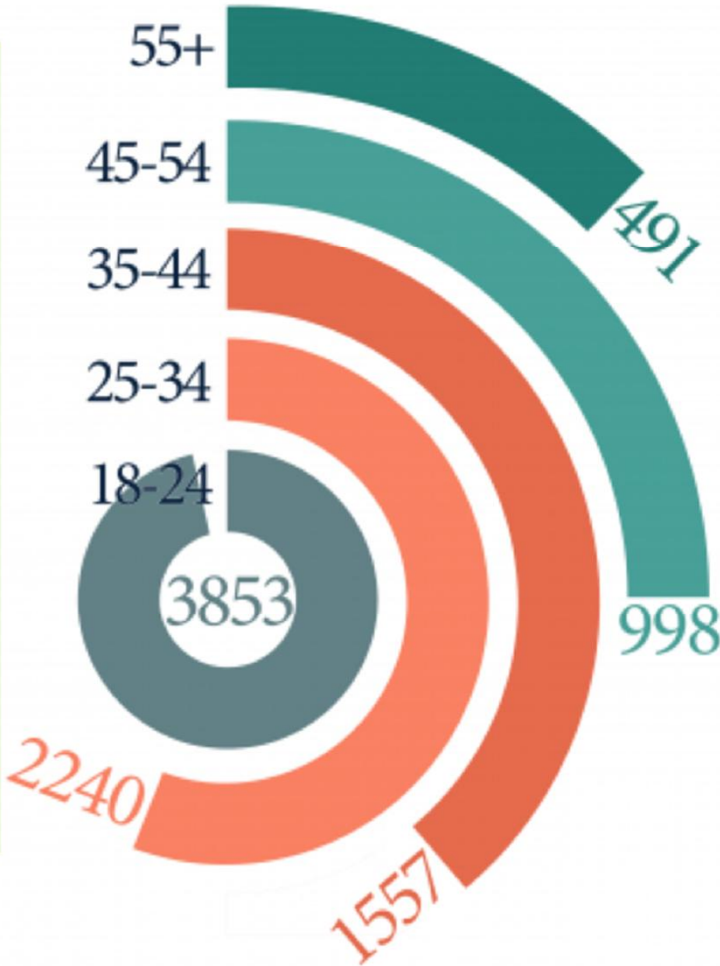


# MOBILE TECHNOLOGY FACTS

Daily Texts by U.S. Adults

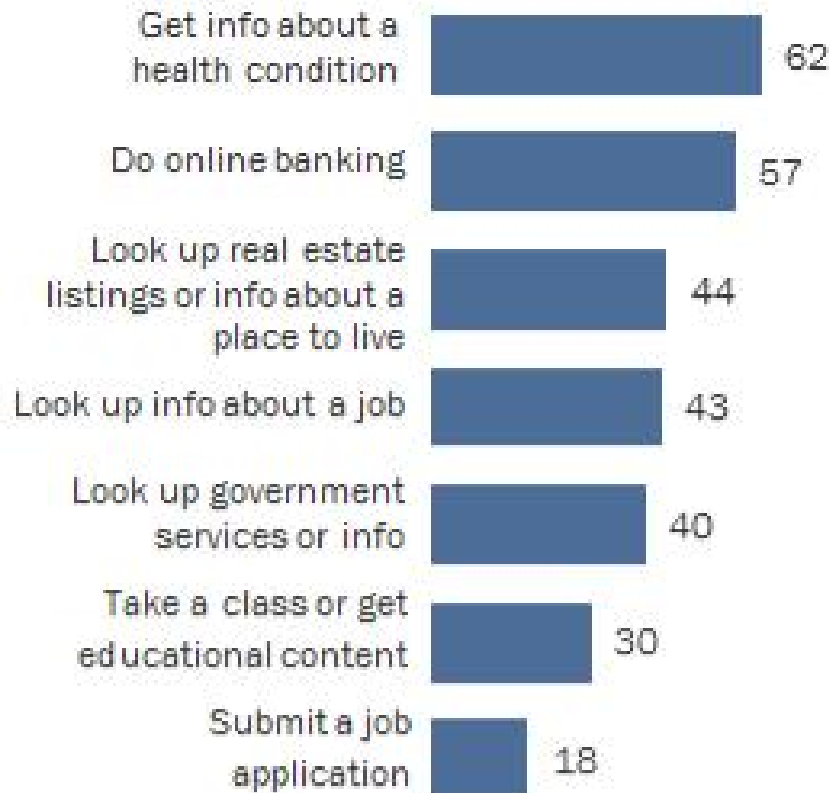


Monthly Texts by U.S. Adults

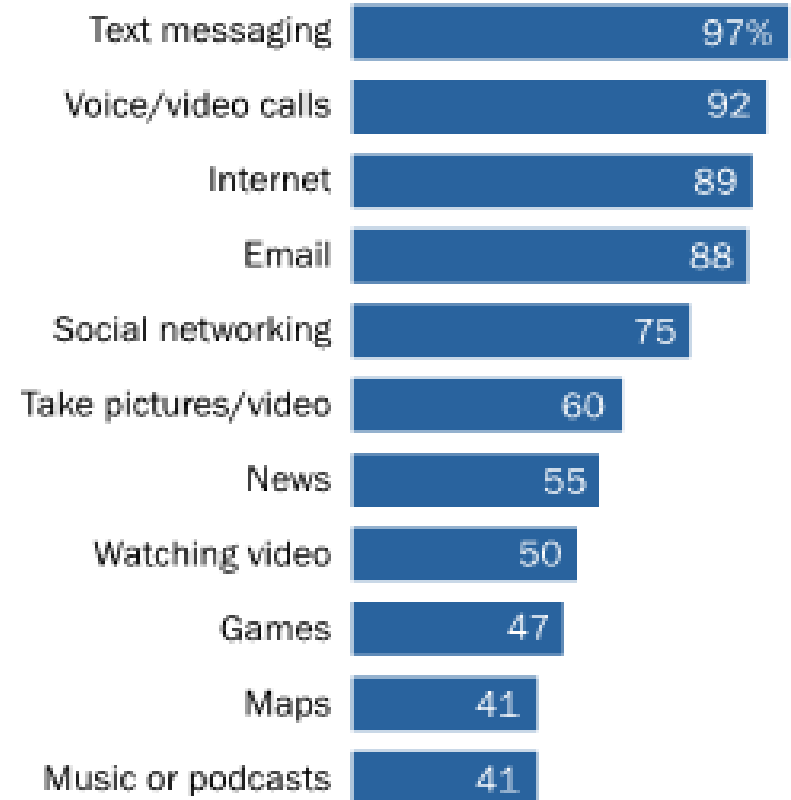


# MOBILE TECHNOLOGY FACTS

*% of smartphone owners who have used their phone to do the following in the last year*



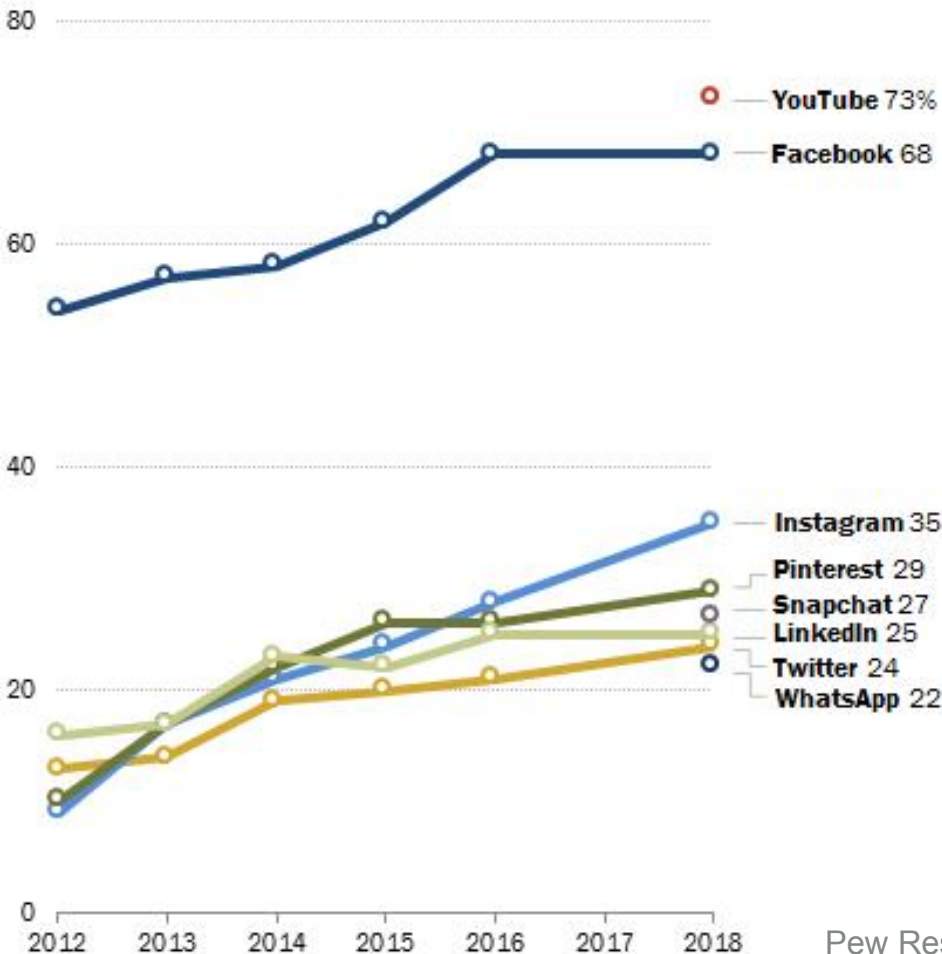
*% of smartphone owners who used the following features on their phone at least once over the course of 14 surveys spanning a one-week period*



# SOCIAL MEDIA FACTS

## Majority of Americans now use Facebook, YouTube

*% of U.S. adults who say they use the following social media sites online or on their cellphone*

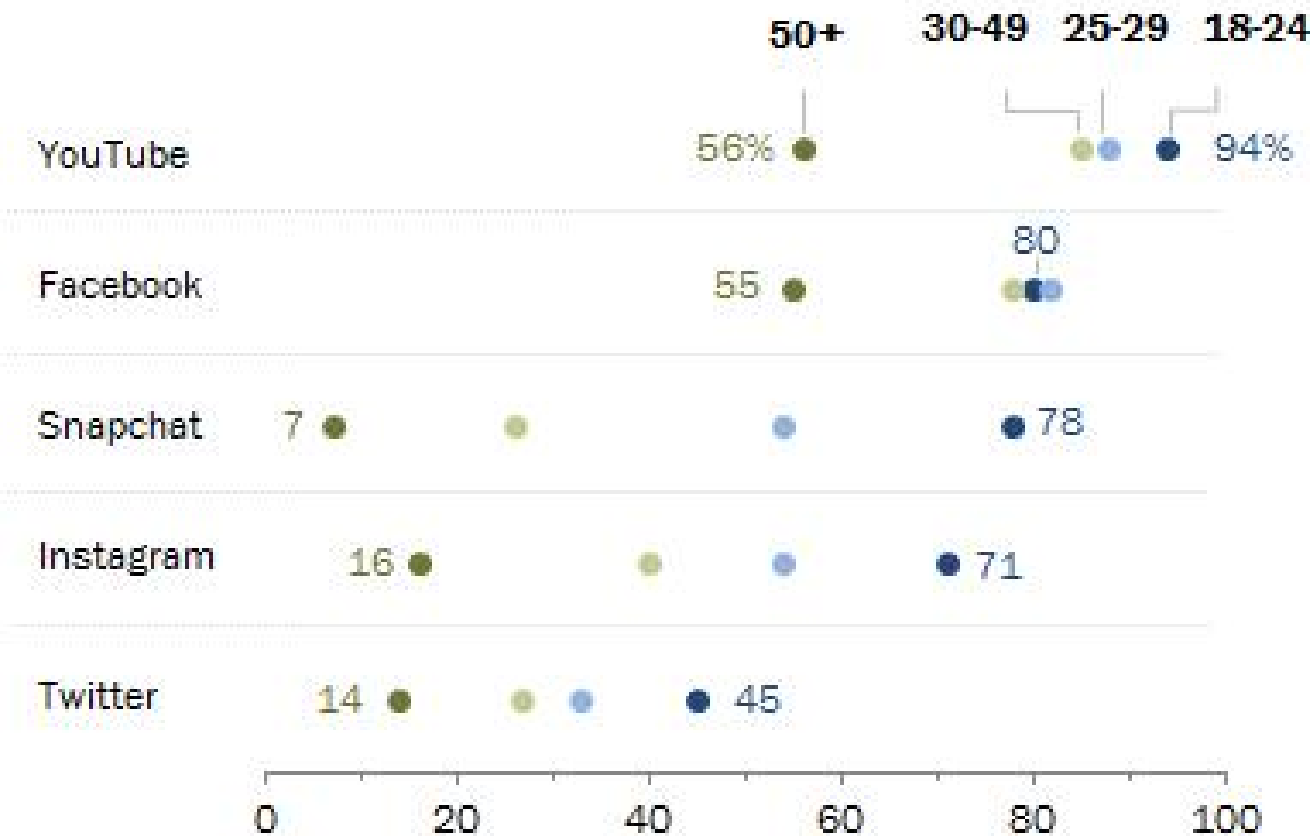




# SOCIAL MEDIA FACTS

## Social platforms like Snapchat and Instagram are especially popular among those ages 18 to 24

*% of U.S. adults in each age group who say they use ...*



Pew Research –

”Social Media Use in 2018

# SOCIAL MEDIA FACTS

## Use of different online platforms by demographic groups

*% of U.S. adults who say they use ...*

	Facebook	YouTube	Pinterest	Instagram	Snapchat	LinkedIn	Twitter	WhatsApp
Total	68%	73%	29%	35%	27%	25%	24%	22%
Men	62	75	16	30	23	25	23	20
Women	74	72	41	39	31	25	24	24
White	67	71	32	32	24	26	24	14
Black	70	76	23	43	36	28	26	21
Hispanic	73	78	23	38	31	13	20	49
Ages 18-29	81	91	34	64	68	29	40	27
18-24	80	94	31	71	78	25	45	25
25-29	82	88	39	54	54	34	33	31
30-49	78	85	34	40	26	33	27	32
50-64	65	68	26	21	10	24	19	17
65+	41	40	16	10	3	9	8	6
<\$30,000	66	68	20	30	23	13	20	20
\$30,000-\$49,999	74	78	32	42	33	20	21	19
\$50,000-\$74,999	70	77	34	32	26	24	26	21
\$75,000+	75	84	39	42	30	45	32	25
High school or less	60	65	18	29	24	9	18	20
Some college	71	74	32	36	31	22	25	18
College+	77	85	40	42	26	50	32	29
Urban	75	80	29	42	32	30	29	28
Suburban	67	74	31	34	26	27	23	19
Rural	58	59	28	25	18	13	17	9

Pew Research –

”Social Media Use  
in 2018

# DO YOU KNOW WHAT THESE APPS ARE?

---



# MOBILE DEVICE AND SOCIAL MEDIA DISCOVERY

---

# LEGAL LANDSCAPE

- ▶ “Electronically Stored Information” includes data stored on mobile devices and social media accounts – if relevant
- ▶ Duty to preserve extends to relevant messages, voicemail, photographs, postings, etc.
- ▶ Parties have been sanctioned for failing to preserve mobile data – adverse inferences and default judgments
- ▶ Privacy, cost/burden, and proportionality concerns are particularly important when it comes to devices and social media



- ▶ Discovery of mobile data limited based on specific needs of case – courts balance benefits of discovery against burdens and expense
- ▶ Discovery should be tailored – entire image of mobile device only allowed in limited circumstances
- ▶ Focus on specific devices and data types
- ▶ Privacy and cost/burden concerns balanced against need for discovery
- ▶ Courts recognize smart phones store “a digital record of nearly every aspect of [the individual’s life].”



- ▶ Often involve individual plaintiffs who are relying on personal devices (mobile phones laptops) to create and store relevant information (text messages, photos, social media posts)
- ▶ Cases typically involve claims of personal injury, harassment, wrongful termination and theft of trade secrets



- ▶ Again, discovery should be tailored. Social media accounts typically contain a tremendous amount of information
- ▶ Be mindful that almost every social media platform has a direct communication aspect
  - ▶ Some emerging platforms are now auto-deleting—e.g., Wickr and Confide
- ▶ Be wary of attempts to circumvent the discovery process by seeking information directly from social media service providers in light of Stored Communications Act





- ▶ The right to inspect, copy, test, or sample ESI is “counterbalanced by a responding party’s confidentiality or privacy interests.”
- ▶ “A party is therefore not entitled to a routine right of direct access to a party’s electronic information system, although such access may be justified in some circumstances.”
  - ▶ *Bakhit v. Safety Marketing, Inc.*, Civ. Action No. 3:13CV1049 (JCH), 2014 U.S. Dist. LEXIS 86761 (D. Conn. June 26, 2014)





- ▶ Use of personal devices for business (BYOD) or personal social media accounts presents some “custody and control” issues
- ▶ Some courts requiring initial showing that specific device is likely to contain relevant information before permitting discovery and the same will likely be the case for social media discovery
- ▶ Definitions of “ESI” in requests tend to be broad – object to mobile or personal (non-business) sources in responses
- ▶ Preservation efforts may not require quarantine of devices – varies by device and facts of case
- ▶ Potential authentication issues

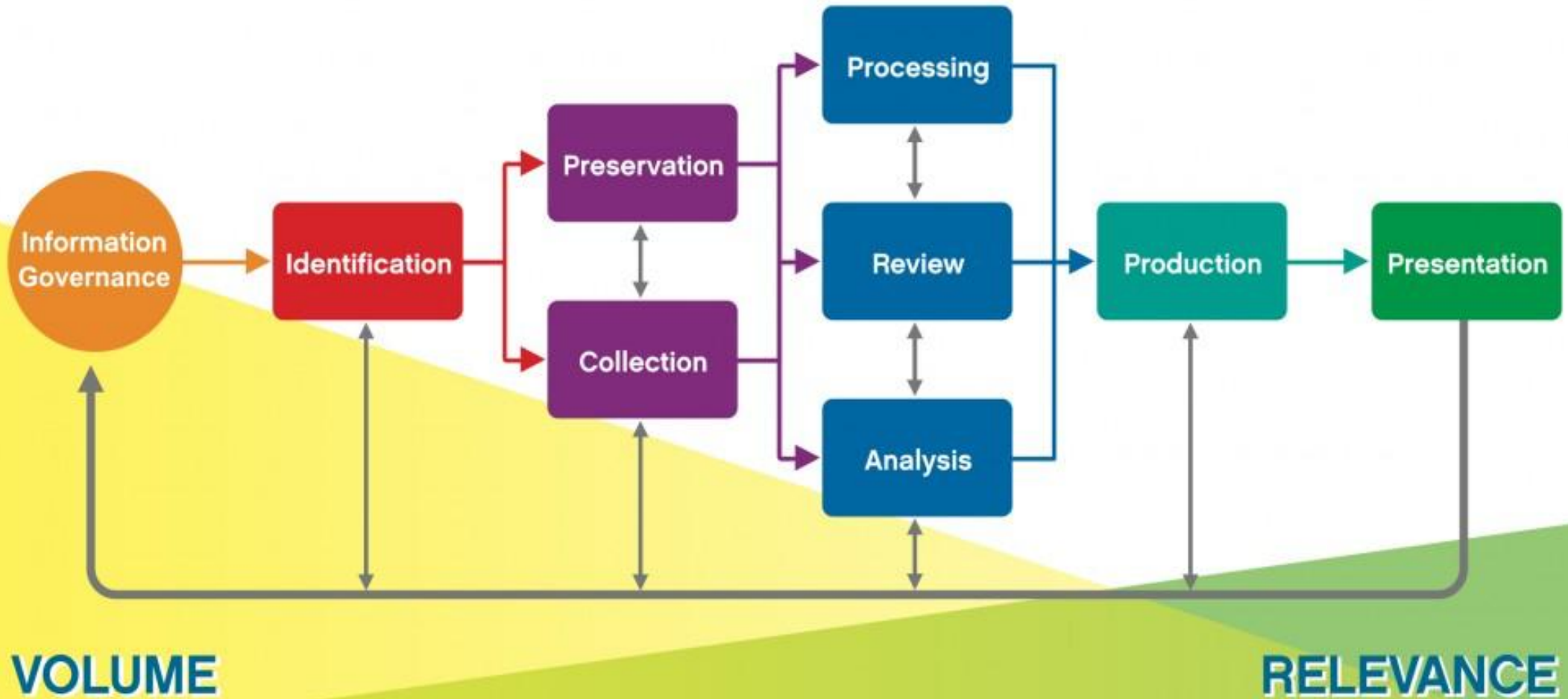
MOBILE DEVICE DISCOVERY:

---

# LEGAL STRATEGIES

# Electronic Discovery Reference Model

20



- ▶ Trust user to comply with hold and understand technical functions and settings on device
- ▶ Collect to preserve
- ▶ Confirm and document no data to preserve
- ▶ The duty to preserve and “no trace” apps, like



and



## MOBILE

- ▶ Physical Capture
- ▶ Logical/Active Capture
- ▶ Direct Access - USB Connection



- ▶ iTunes Backup
- ▶ Backup/Archive Application



SMS Backup & Restore

- ▶ Native Collection Using Built-in Functionality
- ▶ Self Collection



## SOCIAL MEDIA

FORENSIC COLLECTION

“DOWNLOAD YOUR INFO”  
“TWITTER ARCHIVE”

SCREEN SHOTS

SELF COLLECTION

INTERNET ARCHIVE



- ▶ Cost of forensic imaging and professional collection are high
- ▶ Imaging a mobile device requires taking it away from the user and risks collecting private and protected information
- ▶ Personal and business data are commingled on mobile devices
- ▶ BYOD policies need to account for potential need to collect data for discovery



- ▶ Many cases do not discuss actual format for production of mobile device data
- ▶ Mobile data is often not in a traditional document format – Structured data instead
- ▶ Some cases involve protocols specifically addressing process for production – including use of third parties for collection, filtering and production
- ▶ Absent agreement otherwise, Federal Rules require “reasonably useable” format





- ▶ Balance value of information with burdens
- ▶ Proportionality is key
- ▶ Discuss issues and cooperate to handle challenging issues
  - ▶ Front issue in a proposed discovery order
- ▶ Seek court intervention as needed
- ▶ Consult and involve appropriate technologists



MOBILE DEVICE DATA

---

**AUTHENTICATION**


- ▶ Is mobile data what it purports to be?
- ▶ Standards vary by facts and courts
- ▶ Must raise authentication objections or risk waiver



- ▶ Most cases addressing authentication of mobile device data relate to messages in criminal context
- ▶ Issue is often whether particular person received a text/email or whether a particular person sent a text/email



- ▶ Witness with personal knowledge - FRE 901(b)(1)
  - ▶ The Advisory Committee notes explain that “knowledge” is to be liberally construed. Knowledge could be had by the drafter or a recipient of an email, the web-master of a webpage, or by someone who understood the procedure behind the generation of the record.
- ▶ Comparison by trier or expert witness with authenticated documents - FRE 901(b)(3);

- ▶ Distinctive characteristics/circumstantial evidence: appearance, contents, substance, Hash Value - FRE 901(b)(4)
  - ▶ Judge Grimm's 
- ▶ Trade inscriptions FRE 902 (7)
- ▶ Certified copies of business records – FRE 902(11)

## OTHER METHODS OF AUTHENTICATION

---

31

- ▶ Judicial notice
- ▶ Stipulation of parties
- ▶ Request to admit genuineness of documents – FRCP 36
- ▶ Identification of exhibits through pretrial disclosures – FRCP 26(a)(3)



- ▶ Identify types of ESI and strategy for admission in advance
- ▶ Document collection procedures
- ▶ Produce hash values for ESI
- ▶ Track ESI from collection to production
- ▶ Identify necessary witnesses for authentication
- ▶ Consider stipulations and other methods



ALISON GROUNDS – ALISON.GROUNDS@TROUTMANSANDERS.COM

STEPHANIE MITCHELL – STEPHANIE.MITCHELL@SIEMENS.COM

SCOTT WANDSTRAT – SCOTT.WANDSTRAT@AGG.COM

---

# ISSUES AND PRACTICES WITH DEVICES AND SOCIAL MEDIA