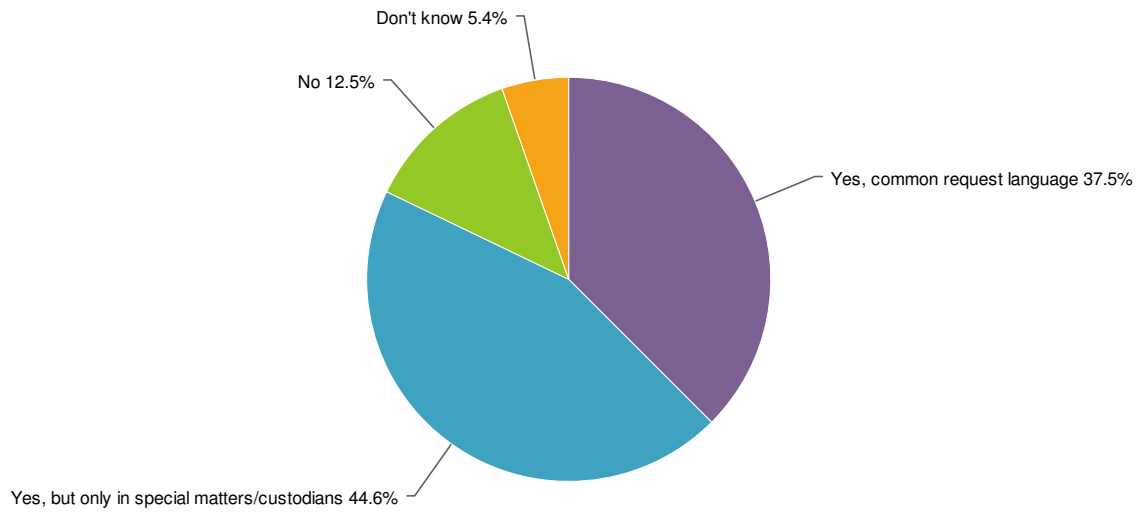
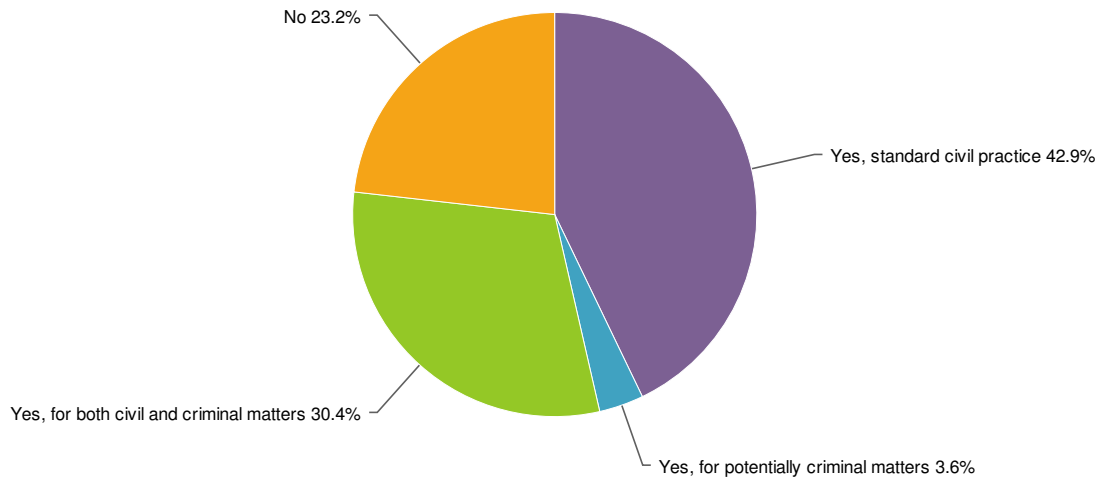


1. Have you ever had ESI from mobile devices requested?



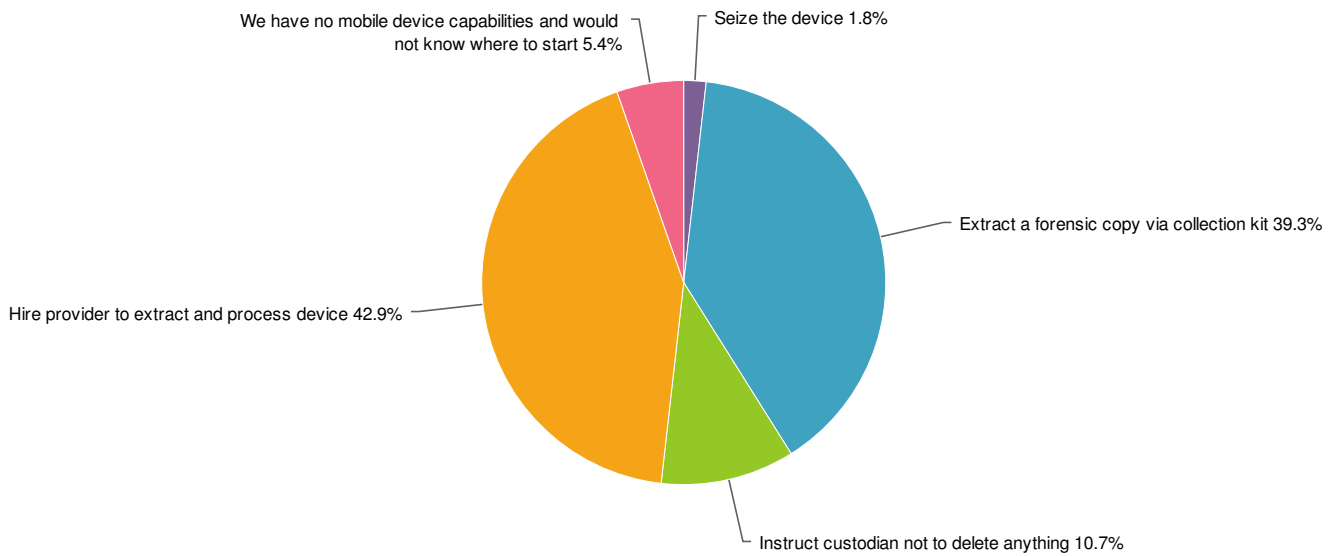
Value	Percent	Count
Yes, common request language	37.5%	21
Yes, but only in special matters/custodians	44.6%	25
No	12.5%	7
Don't know	5.4%	3
	<b>Total</b>	<b>56</b>

## 2. Have you ever had to preserve or collect ESI from a custodian's mobile device?



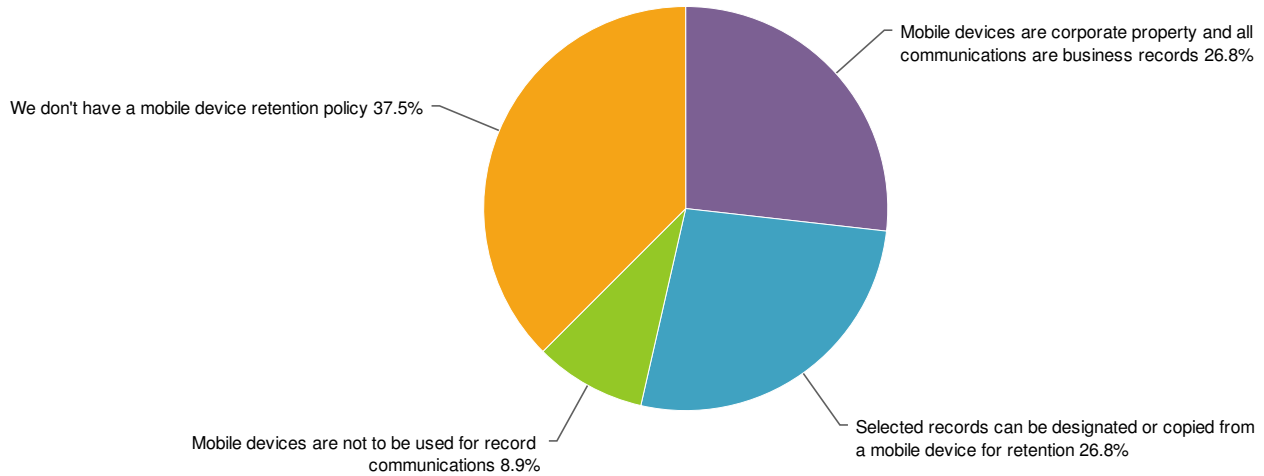
Value	Percent	Count
Yes, standard civil practice	42.9%	24
Yes, for potentially criminal matters	3.6%	2
Yes, for both civil and criminal matters	30.4%	17
No	23.2%	13
Total		56

### 3. How would you preserve/collect from a mobile device?



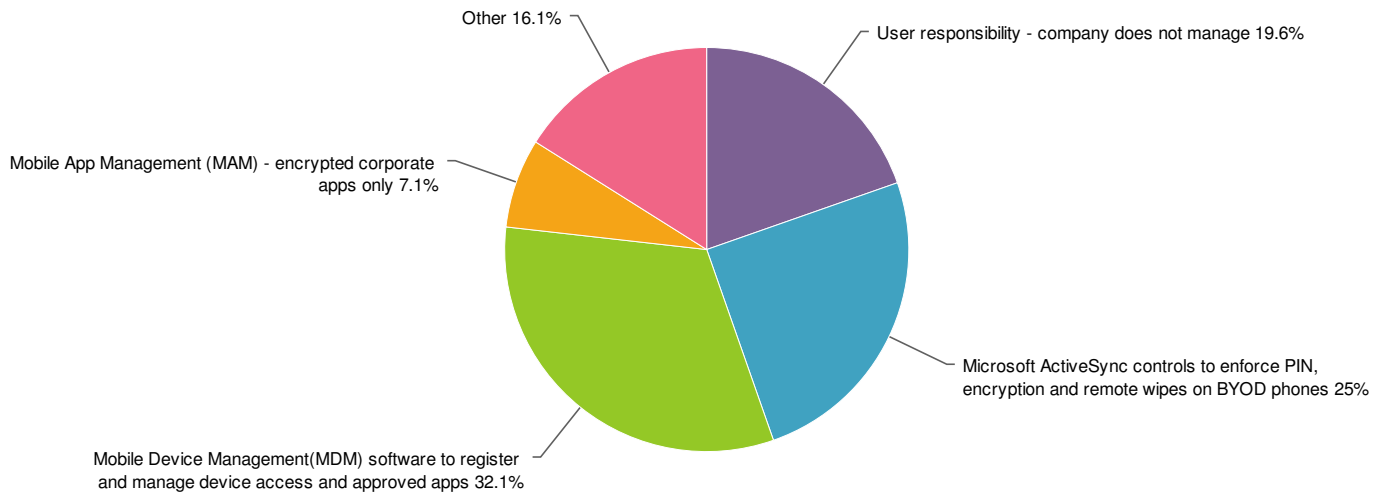
Value	Percent	Count
Seize the device	1.8%	1
Extract a forensic copy via collection kit	39.3%	22
Instruct custodian not to delete anything	10.7%	6
Hire provider to extract and process device	42.9%	24
We have no mobile device capabilities and would not know where to start	5.4%	3
<b>Total</b>		<b>56</b>

#### 4. What is your retention policy for mobile devices?



Value	Percent	Count
Mobile devices are corporate property and all communications are business records	26.8%	15
Selected records can be designated or copied from a mobile device for retention	26.8%	15
Mobile devices are not to be used for record communications	8.9%	5
We don't have a mobile device retention policy	37.5%	21
	Total	56

## 5. How do you manage mobile device access and security?



Value	Percent	Count
User responsibility - company does not manage	19.6%	11
Microsoft ActiveSync controls to enforce PIN, encryption and remote wipes on BYOD phones	25.0%	14
Mobile Device Management(MDM) software to register and manage device access and approved apps	32.1%	18
Mobile App Management (MAM) - encrypted corporate apps only	7.1%	4
Other	16.1%	9
Total		56