1.

(a)

Differential privacy. Add noise while collecting lifespan information can protect the users' privacy.

(b)

Secure multiparty computation. Both party wants the information about combining their own information with the other while keeping theirs in secret. Only secure multiparty computation supports it.

(c)

Private information retrieval. You don't want the data owner to get any knowledge about you, which is supported by PIR.

(d)

Differential privacy. Add some noise to your query and send it to the server. So that the server will not know where exactly you are.

2.

Sun	Mon	Tue	Wed	Thu	Fri	Sat
Full	differential	differential	differential	Inc	Inc	inc

In a day,

- p% of files are changed.
- D amount of data
- needs to store k bits of change

(a)

Mon	D*p
Tue	2*D*p
Wed	3* D*p
Thu	D*p
Fri	D*p
Sat	D*p
Sun	D

Wednesday's partial backup is the largest.

(b)

Tuesday and Wednesday can be different. as files might be changed twice, the p portion of file being changed on Monday can also be the same files being changed on Tuesday and Wednesday. As a result, the mean of expected storage for Tuesday and Wednesday are expected to be different from (a).

The largest partial backup can be different as well. Wednesday can be modifying the same files as Tuesday.

So the possible answers to largest partial backup are:

a. Wednesday
b. Tuesday and Wednesday

c. Monday to Saturday are all the same

(c)

Thursday's backup was corrupted. Since Thursday, Friday and Saturday are using incremental backup, if Thursday's backup is compromised, all the backups following it will be affected as well. Therefore, 3 days of backup cannot be restored due to the corruption of Thursday's backup.

(d)
If it is hashed, then there is no way to recover the data back as hash is a one-way function.

3.
(a)
expected cost for winning a hash:
10000 + (1 * 600) * 100 (expected times to win) = $70000

70000/ 12 ~= 5833 ($/Bitcoin)
(b)
1 block <= 1024 * 1024 bytes
1 transaction >= 166 bytes
1 block at most 6316 transactions
1 block every 600 seconds
6316 / 600 ~= 10 transactions/ second

(c)
According to (b), there are at most 10 (transactions/ second)
According to (a), the expected cost for winning a hash is $70000

Assume uniform distribution, the mean number of transaction/ block is 3158.
If the price stays the same, but the reward decreased to 6 Bitcoin, you need to cover the half of the cost with transaction fee.
Therefore, transaction fee is 70000/2/3158 ~= $111 for each transaction

(d)

Let x be the number of devices to be bought.

Cost:
x * 10000 + 365 * 24 * 3600 * x = 31546000 * x

Revenue:
Chance of winning the hash = (x/100)
Number of hash per year = 360 * 24 * 60 / 10 = 51840 hashes
Expected revenue = 51840 * (x/100) * 12 * 10000 ~=62160000* x

62208000 * x - 31546000 * x >= 1000000
x>= 1

You should at least buy one machine.