WORKPLACE PRIVACY & ETHI

MODULE 4

Work place monitoring

- Keeping an eye on employees
- Monitoring will be done on quantity and quality of work produced by their emplo
- Employees has some degree of privacy in workplace.
- Excessive, routine and unnecessary mon is a breach of data protection laws

Need of workplace monitori

- Employee or customer safety
- Liability & investigations- harrassments,the
- Network and system perf.:protection a virus, avoiding network slowdown etc
- Right to know for employers: legitimate pro
- To check the procedure are following
- To prevent or detect crime
- In the interest of national interest

Types of work place monitori

- Hardware monitoring
- Software monitoring

Hardware monitoring

- Audio surveillance
- Video surveillance
- Infrared badges at work
- Mega stripe cards

Software monitoring

- Electronic surveillance
- Spyware
- Screen, data, idle time monitoring

Advantages

- Reduce mistake
- Employee safety
- Unbiased performance evaluation
- Violation of policies prevented

Disadvantages

- Prevents efficiency-being too intrusive
- Expensive instrument
- Devious employees
- Too much monitoring lead to high infide
  competition rather than team competiti
- Too much monitoring lead discomfort of
  employee

Computer crime

- Type of fraud where computers are used
- It is a an act performed by a knowledgea user.

- Ex: unlawful use or access- hacking(wi permission)
- access for fraud
- Data theft- use/ copy/damage/ alter info permission

Computer crime at workplac

- Computer crime in increasing in workpla
- Use of authorisation to get a sensitive da change it or sell it to make more money
- Most fraud are not committed employee
-

Types of computer crimes at workplace

- Software theft - theft-unlicensed copying
- Hardware theft - microprocessors, laptop hard disk drives etc
- Hardware theft is most common fraud

Preventing computer crimes a workplace

- Tactic such as encryption, firewalls, emp training and awareness, routine audit, ph surveillance, appointing security personn

- Reward system for employees for report employee initiated audit, updating comp virus program, ISO agreements etc

Workplace plagiarism

- Act of fraud
- Involves both stealing someone's work a lying about it afterward

Types of workplace plagiaris

- Using others' images & work
- Taking credit for an idea
- Failing to list a source
- Stealing blog content
- Reproducing an e-book

Effect of workplace plagaris

- Personal integrity
- Legal consequences
- Company reputation
- Fairness to colleagues

Employee privacy and ethics (i

- Freedom for employee from unauthorise intrusion from employers

- Describes the context to which employer monitor ad collect information on the activities, communication, and private liv workers.

- A controversial and legal issue
- Employers are allowed
- Other pvt spaces- lockers/ drawers- e/rs should not violate worker's privacy
- Tough task-to decide how much monitor necessary?

No privacy but convenience

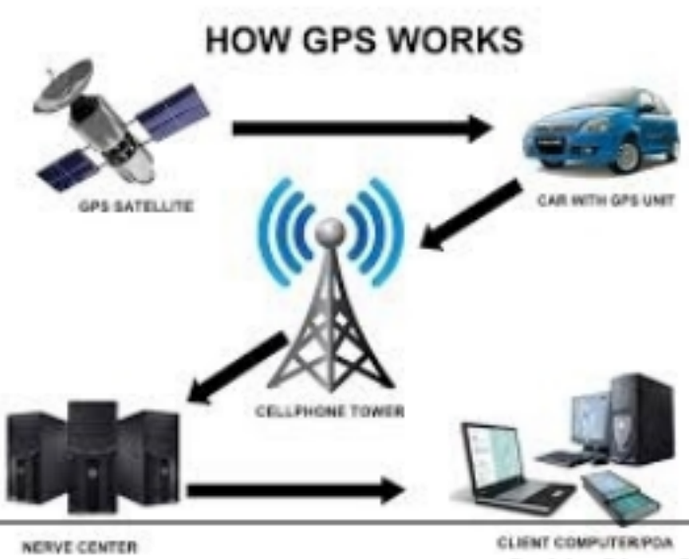
A debate…

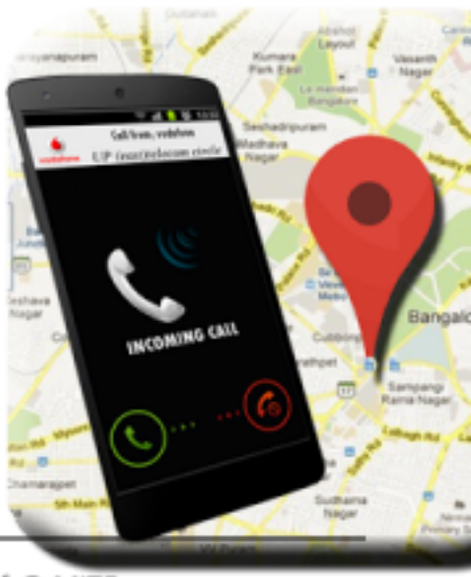
- Would you like to have complete privacy workplace but accept the risk of pot abuse/ other problems??
- Are you ready to give away ur privacy fo benefit of avoiding any problems?

Death of privacy

- Digital footprints- to track what employe
  delivery records, travel logs, expense rep
  productivity reporting etc
- Electronic toll collection tags- to record
  passing time in vehicle without stopping th
- Cell phones- monthly bill can be reviewed
- Even location from where the calls were re
  made could be traced- transmission towers
- GPS- should not track e/e s location afte
  hours-unfair to do so. (global positioning sy

Use all the above with legitimate business rea





Defence of employee privacy ri

- employers not to intrude employees per life, choices, background, habits etc.
- Without considering the employees inte not to be disclose/discussed in public
- Ex.: pvt msgs in inbox, checking purses/w in public
- When employee not trusted he/she wou longer see any incentive in being produc /efficient

- Increased surveillance leaves no room fo
  employee self control and self monitorin

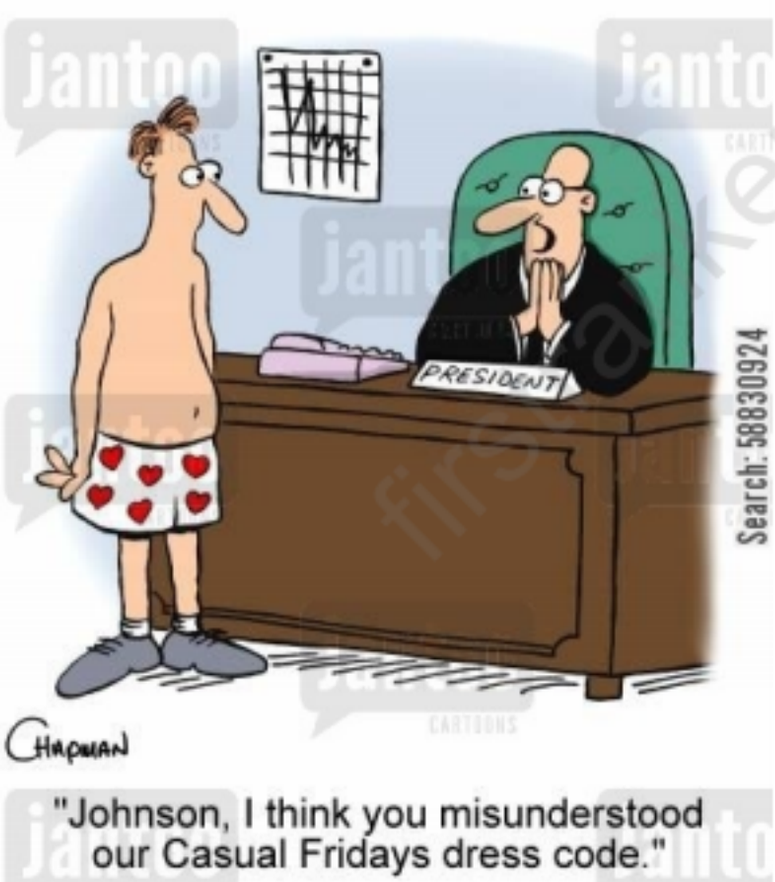
- With data security and other organisatio
  interests becoming paramount, the emp
  rights for privacy and freedom is curtaile

Breaching employee privac

- During recruitment process - confidential info li family background etc- if relevant but to be kept confidential in co records
- During performance tracking - to check work ha client management to find causes for poor perfo etc
- During electronic surveillance - necessary to kee check on the work space activities
- Electronically stored e/e data- getting access to people- personal and professional data must be confidential.

Guidelines to defend employee pr

- Let there be a clear policy- taking consent and makir aware of what is pvt and what is not
- Only on legal grounds-no other utility of the mor tools
- Do not have unnecessary harsh policies- result in att
- No electronic harassment – offensive emails/dirt take enough care
- Use of internet only for business
- Use of all electronic tools for business or profe purpose
- In-house privacy controller- for large orgtns can be rep for data protection and use of techno in the org



"Johnson, I think you misunderstood our Casual Fridays dress code."