Professional Issues Professions and Professionals

PROFESSIONS AND PROFESSIONALS

- What is a profession
- Professional Conduct
- Professional bodies in Computing
- Computer Misuse

The Bell Pottinger Case

Bell Pottinger was expelled on Monday from the UK's Public Relations and Communications Association (PRCA), which decided the campaign it ran for the Guptas – a family of Indian-born tycoons who are close to president Jacob Zuma – "was by any reasonable standard of judgment likely to inflame racial discord in South Africa".

South Africa's main opposition party, the Democratic Alliance (DA), had complained to the PRCA about the campaign, which portrayed opponents of President Zuma as agents of "white monopoly capital" and coined slogans referring to "economic apartheid".

2 Conduct towards the Public, the Media and other Professionals

A member shall:

2.1 Conduct their professional activities with proper regard to the public interest.

2.2 Have a positive duty at all times to respect the truth and shall not disseminate false or misleading information knowingly or recklessly, and to use proper care to avoid doing so inadvertently.

2.3 Have a duty to ensure that the actual interest of any organisation with which they may be professionally concerned is adequately declared.

2.4 When working in association with other professionals, identify and respect the codes of these professions and shall not knowingly be party to any breach of such codes.

2.5 If a member of either House of Parliament, member of a Local Authority or of any statutory organisation or body, record that material in the relevant section of the PRCA Public Affairs and Lobbying Register.

2.6 Honour confidences received or given in the course of professional activity.

2.7 Neither propose nor undertake any action which would constitute an improper influence on organs of government, or on legislation, or on the media of communication.

2.8 Neither offer nor give any inducement to persons holding public office or members of any statutory body or organisation who are not directors, executives or retained consultants, with intent to further the interests of the organisation if such action is inconsistent with the public interest.

THE UNIVERSITY of EDINBURGH informatics

1. On your own: write a definition of the meaning of "profession" (2 or three lines max).

2. In a pair:

   ■ compare and discuss your definitions – do they capture what you want to capture?

   ■ If they differ significantly keep both and refine them, otherwise produce a single refined definition

3. In fours: combine your definitions into at most two definitions: main and alternate.

Pause – While we do the task in hand

Profession

Wikipedia: "A **profession** is a vocation founded upon specialised educational training, the purpose of which is to supply disinterested counsel and service to others, for a direct and definite compensation, wholly apart from expectation of other business gain" (New Statesman, 21 April 1917)

Have a look at the Wikipedia page because it is contested precisely on the distinction between the vernacular and technical meanings.

What Makes a Profession?

"To me, the essence of professionalism is a commitment to develop one's skills to the fullest and to apply [them] responsibly to the problems at hand. Professionalism requires adherence to the highest ethical standards of conduct and a willingness to subordinate narrow self-interest in pursuit of the more fundamental goal of public service"

Justice Sandra Day O'Connor - US Supreme Court

Some other definitions…

"Doing things right and doing the right thing" *(Chambers 20th Century Dictionary)*

"an employment not mechanical and requiring some degree of learning; habitual employment; the collective body of persons engaged in any profession …"

(lawyers, doctors, architects, surveyors, accountants, engineers,etc)

the collective body controls entry to the profession;

the collective body is self governing and self regulatory, in the sense that it establishes and enforces a code of conduct on its members;

the collective body is established either by a Royal Charter or an Act of Parliament which defines the extent of its authority and requires it to undertake certain duties and responsibilities.

Professional Bodies

Promote and set standards in education

    Accredit courses

Promote continuing personal development

Promote advancement of the subject

Promote exchange of knowledge

Give official advice

Term "engineer" much more strictly applied than here

State licensing boards

Applying strict regulation to software engineers would cripple the sector

Professional Issues:
Meeting 1 Professionalism

of **Conduct**

Sets out the professional standards required by the Society as a condition of membership

Covers public interest, duty to relevant authority, duty to the profession, professional competence and integrity

of **Good Practice**

"describes standards of practice relating to contemporary demands found in IT"

Covers practices common to all disciplines plus some specific to IT, business, education .. Such as:

1. Public Interest

You shall:

have due regard for public health, privacy, security and wellbeing of others and the environment.

have due regard for the legitimate rights of Third Parties*.

conduct your professional activities without discrimination on the grounds of sex, sexual orientation, marital status, nationality, colour, race, ethnic origin, religion, age or disability, or of any other condition or requirement

promote equal access to the benefits of IT and seek to promote the inclusion of all sectors in society wherever opportunities arise.

2. Professional Competence and Integrity

You shall:

only undertake to do work or provide a service that is within your professional competence.

NOT claim any level of competence that you do not possess.

develop your professional knowledge, skills and competence on a continuing basis, maintaining awareness of technological developments, procedures, and standards that are relevant to your field.

ensure that you have the knowledge and understanding of Legislation* and that you comply with such Legislation, in carrying out your professional responsibilities.

respect and value alternative viewpoints and, seek, accept and offer honest criticisms of work.

avoid injuring others, their property, reputation, or employment by false or malicious or negligent action or inaction.

reject and will not make any offer of bribery or unethical inducement.

The General Data Protection Regulation

GDPR provides the following rights for individuals:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

When does the right apply?

Individuals have the right *not to be subject to a decision* when:

- it is based on automated processing; and
- it produces a legal effect or a similarly significant effect on the individual.

You must ensure that individuals are able to:

- obtain human intervention;
- express their point of view; and
- obtain an explanation of the decision and challenge it.

Does the right apply to all automated decisions?

No. The right does not apply if the decision:

- is necessary for entering into or performance of a contract between you and the individual;
- is authorised by law (eg for the purposes of fraud or tax evasion prevention); or
- based on explicit consent. (Article 9(2)).

Furthermore, the right does not apply when a decision does not have a legal or similarly significant effect on someone.

What else does the GDPR say about profiling?

The GDPR defines profiling as any form of automated processing intended to evaluate certain personal aspects of an individual, in particular to analyse or predict their:

- performance at work;
- economic situation;
- health;
- personal preferences;
- reliability;
- behaviour;
- location; or
- movements.

When processing personal data for profiling purposes, you must ensure that appropriate safeguards are in place.

You must:

- Ensure processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the envisaged consequences.

- Use appropriate mathematical or statistical procedures for the profiling.

- Implement appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors.

- Secure personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

1. Individually, do you know any systems that you use that apparently break the GDPR rules on decision making?

2. In pairs, which part of the code of conduct do you think this causes most problem with?

Professional Issues:
Meeting 1 Professionalism

Pause while we do the exercise

Professional Issues:
Meeting 1 Professionalism

International Federation for Information Processing

"the leading multinational, apolitical organization in Information & Communications Technologies and Sciences

recognized by United Nations and other world bodies

represents IT Societies from 56 countries or regions, covering all 5 continents with a total membership of over half a million

links more than 3500 scientists from Academia and Industry, organized in more than 101 Working Groups reporting to 13 Technical Committees

sponsors 100 conferences yearly providing unparalleled coverage from theoretical informatics to the relationship between informatics and society including hardware and software technologies, and networked information systems"

THE UNIVERSITY *of* EDINBURGH
informatics

Why might that be?

IFIP: no Code of Conduct

Attempts were criticised as being from the perspective of white well-off males.

Instead it issued guidelines but left this to member organisations

E.g. on viruses: IFIP urges:

Computer professionals to recognise the disastrous potential of viruses and not to distribute viruses knowingly

Educators to impress upon students the dangers of viruses

Publishers to refrain from publishing details of virus programs

Developers of virus detectors not to distribute viruses as tests

Resources to be devoted to R & D of protection mechanisms

Governments to make distribution an offence

As an ACM member I will:

Contribute to society and human wellbeing

Avoid harm to others

Be honest and trustworthy

…

Mobility directives

Allow movement and professional recognition between countries

Fédération Européene d'Associations Nationales d'Ingénieurs

Members can use prefix Eur.Ing.

Professional Issues:
Meeting 1 Professionalism

Maintain your technical competence

Adhere to regulations

Act professionally as a specialist

Use appropriate methods and tools

Manage your workload efficiently

Participate maturely

Respect the interests of your customers

Promote good practices within the organisation

Represent the profession to the public

Information Technology
Programme/Project Management
Relationship Management
Security and Safety
Change Management
Quality
Business Processes
Research & Development

We'll Look at these in more detail later

Summary

Members of the Computing Profession are expected:

    to work within the relevant legal framework

    to act within a framework of rules of conduct

    to be familiar with best practice and to exercise judgement in applying it

Important documents to read are

    Bott et al. Chapter 1-3

    BCS Code of Conduct

    BCS Code of Good Practice

Homework for next time:

    Write a paragraph contrasting the Code of Conduct with the Code of Practice. In particular invent two example contexts – one where the CoC is more useful than the CoP and vice versa.

No man is an island…

Professional Issues

ethical, legal, economic, organisational and social issues that affect the practice of informatics

even the smartest technology is an executed program unconcerned with ethics, morals, and political debate

Small Stellated Dode...

Social Justice Framework

Distributive justice

Equity
Equality
Need

Self-Interest
Efficiency
Fairness

Voice
Participation

Consistency
Ethicality
Impartiality
Accuracy
Error Correctability

Trust
Dignity
Respect

Procedural justice

Representativeness

Information
Feedback
Explanations

Interactive justice
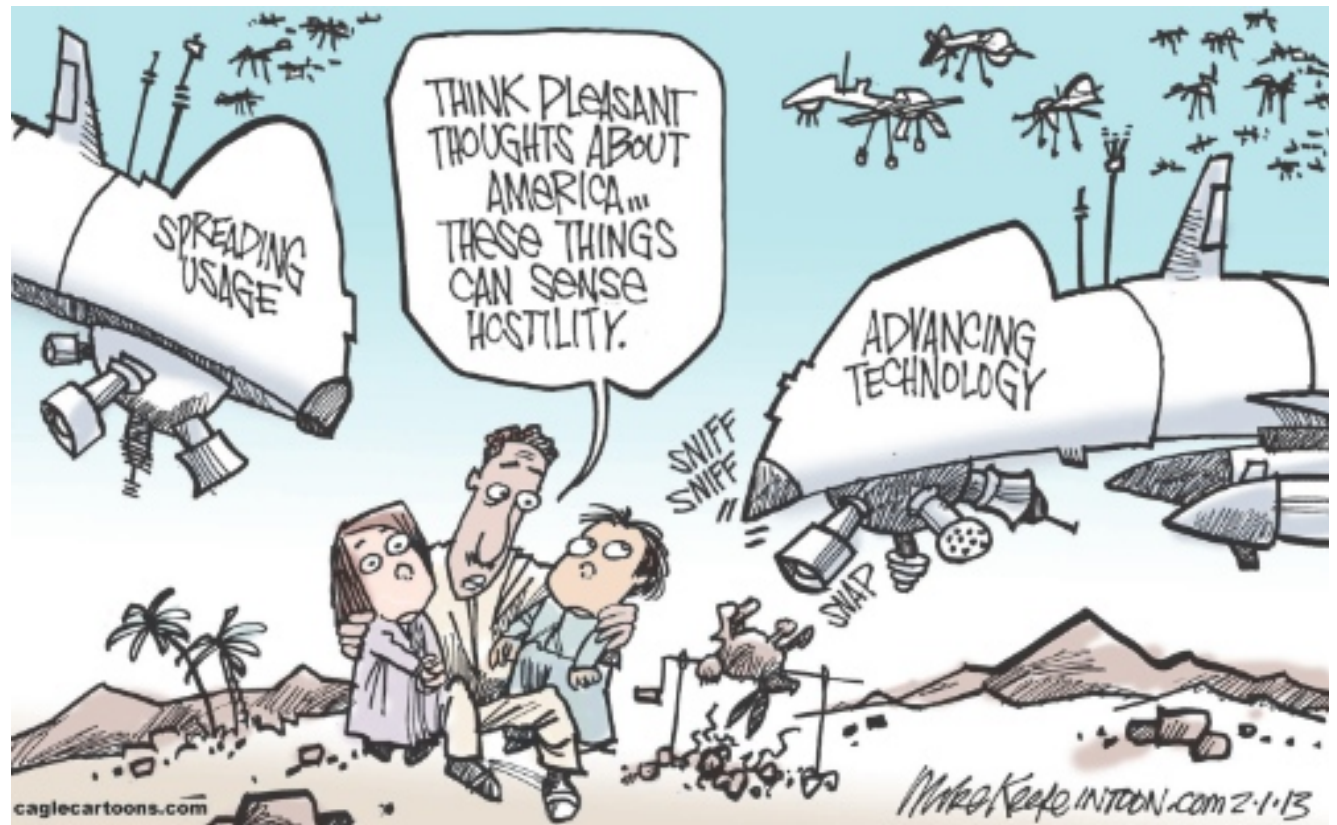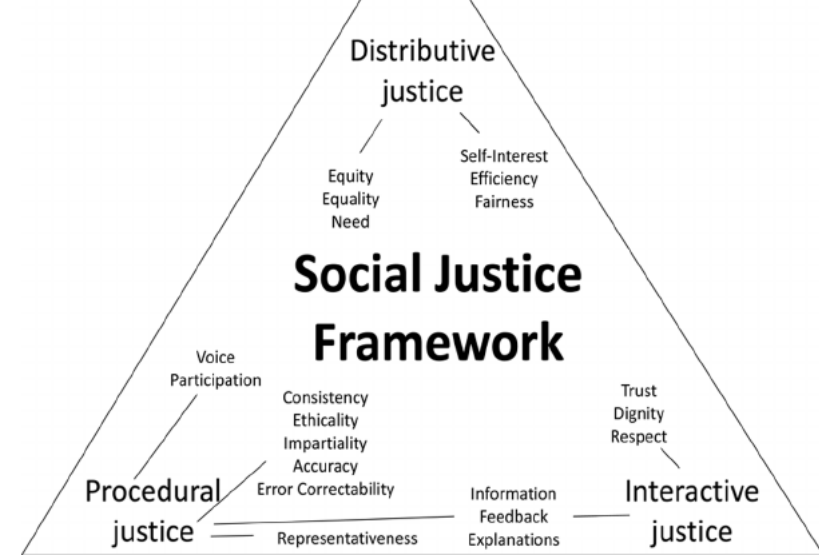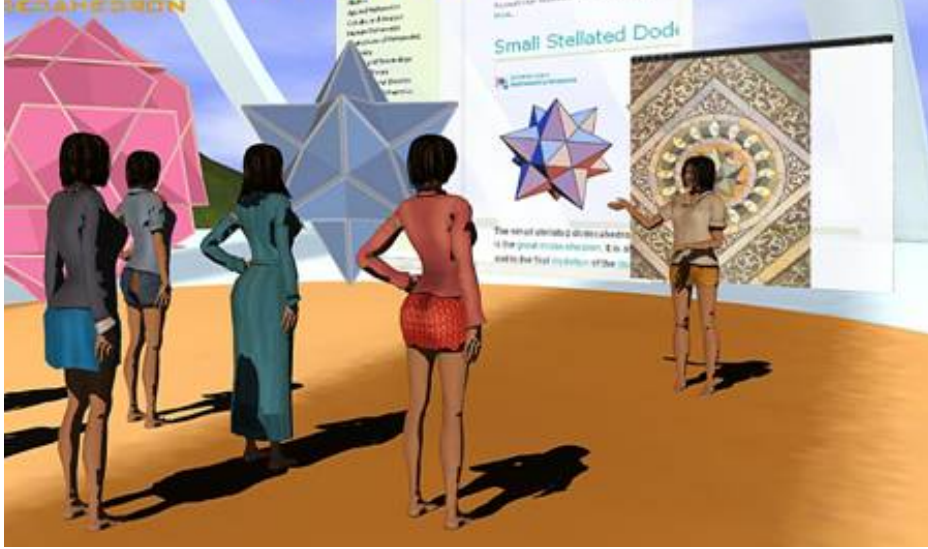
- The social, economic, moral, and legal frameworks that shape the software ecosystem.

- Architectures, operating systems, programming languages, applications, companies and individuals rise and fall.

- Society guarantees some rights, and imposes many responsibilities and obligations.

- Non-technical forces will play a role in shaping what you can achieve.

- To understand some of these forces may be helpful.

Government and Law

Computing Profession

ompanies and Organisations

Finance Accounting and Investment

Human Resources and Discrimination

HR SAY WE SHOULD BE LOOKING FOR A LITTLE FRESH BLOOD ANY IDEA WHAT THEY'RE TALKING ABOUT?

IPR, Software Contracts, Data Protection, Privacy

11 INTELLECTUAL PROPERTY RIGHTS
11.1 INTELLECTUAL PROPERTY
11.2 COPYRIGHT
11.3 EXAMPLES OF COPYRIGHT CASES INVOLVING SOFTWARE
11.4 CONFIDENTIAL INFORMATION
11.5 PATENTS
11.6 TRADE MARKS
11.7 DOMAIN NAMES

12 SOFTWARE CONTRACTS AND LICENCES
12.1 WHAT IS A CONTRACT?
12.2 LICENCE AGREEMENTS
12.3 OUTSOURCING
12.4 CONTRACTS FOR BESPOKE SOFTWARE
12.5 CONTRACTS FOR CONSULTANCY AND CONTRACT HIRE
12.6 LIABILITY FOR DEFECTIVE SOFTWARE
12.7 HEALTH AND SAFETY

13 DATA PROTECTION, PRIVACY AND FREEDOM OF INFORMATION
13.1 BACKGROUND
13.2 DATA PROTECTION
13.3 PRIVACY
13.4 FREEDOM OF INFORMATION

The Internet, Defamation, Pornography, Spam

Computer Misuse and Fraud
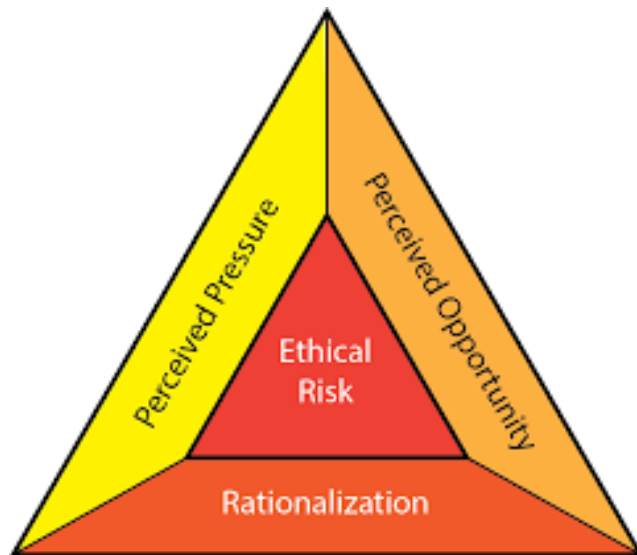
Cloud use questioned over PRISM leaks

The rise of cloud computing – with millions of people storing data on servers in the United States – enabled vast amounts of personal data to be collected by the U.S. National Security Agency's PRISM programme

1 Internet user: Data travels through wire, fibre-optic networks, and undersea cables to telecom companies in United States

Email   *Phone calls**   *Images*   *Video*

2 Telecom company — Data routed to fibre-optic splitter

3 PRISM: Uses phone-billing software to analyse types of data sent – email, video, or voice traffic. PRISM said to handle 2.5 gigabits of data per second

PRISM allegedly used at between 10 and 20 secret centres since 2007

YAHOO!
Microsoft

Cloud

4 NSA interception
Duplicates of all cloud traffic – emails, attachments, web pages and VoIP phone calls – routed to NSA

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

*including voice over internet protocol calls (VoIP)

(TS//SI//NF) Introduction

U.S. as World's Telecommunications Backbone

PRISM

- Much of the world's communications flow through the U.S.

- A target's phone call, e-mail or chat will take the **cheapest** path, **not the physically most direct** path – you can't always predict the path.

- Your target's communications could easily be flowing into and through the U.S.
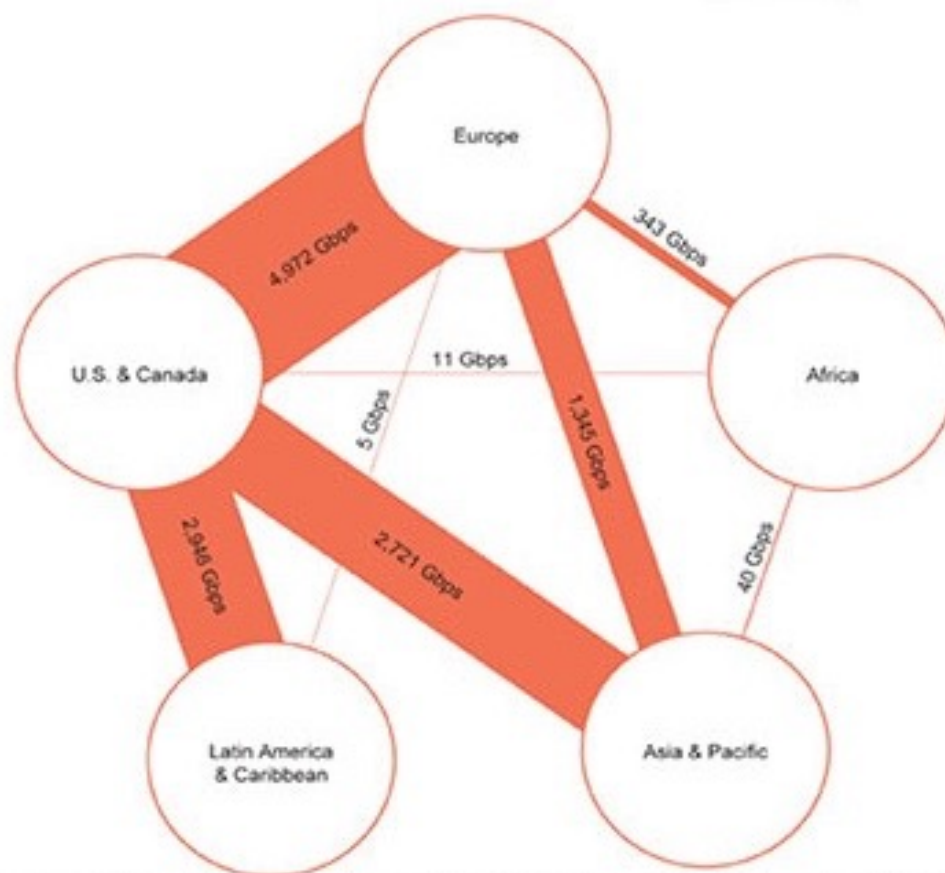
International Internet Regional Bandwidth Capacity in 2011
Source: Telegeography Research

(TS//SI//NF) PRISM Collection Details

PRISM

Current Providers

- Microsoft (Hotmail, etc.)
- Google
- Yahoo!
- Facebook
- PalTalk
- YouTube
- Skype
- AOL
- Apple

What Will You Receive in Collection (Surveillance and Stored Comms)?
It varies by provider. In general:

- E-mail
- Chat – video, voice
- Videos
- Photos
- Stored data
- VoIP
- File transfers
- Video Conferencing
- Notifications of target activity – logins, etc.
- Online Social Networking details
- **Special Requests**

Complete list and details on PRISM web page:
Go PRISMFAA
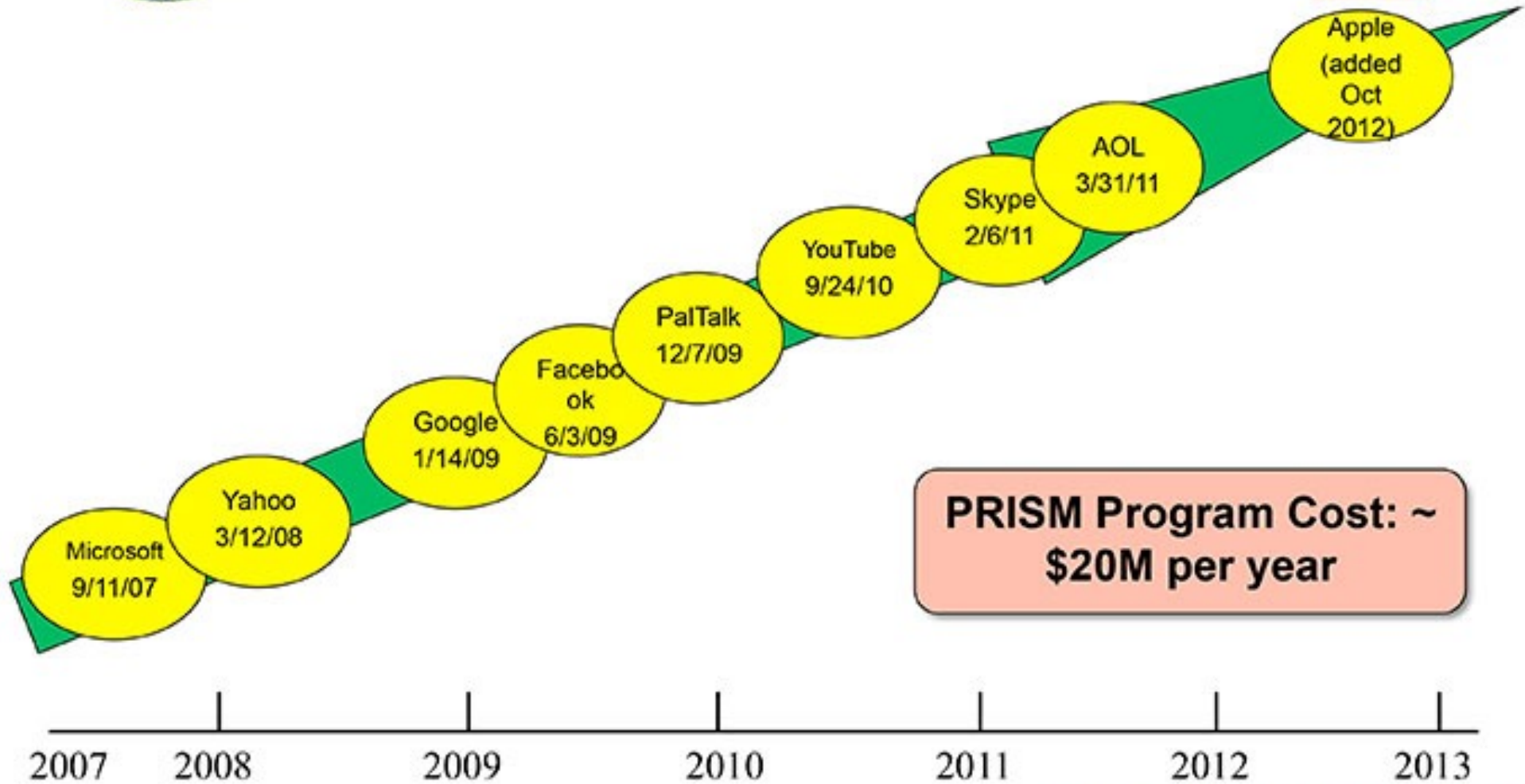
"ARGUING THAT YOU DON'T CARE ABOUT THE RIGHT TO PRIVACY BECAUSE YOU HAVE NOTHING TO HIDE IS NO DIFFERENT THAN SAYING YOU DON'T CARE ABOUT FREE SPEECH BECAUSE YOU HAVE NOTHING TO SAY."

-Edward Snowden

Straw Poll

Government and Law		
Computing Profession		
Companies and Organisations		
Finance Accounting and Investment		
Human Resources and Discrimination		
IPR Software Contracts, Data Protection, Privacy		
The Internet Defamation, Pornography, and Spam		
Computer Misuse and Fraud		
Surveillance and Encryption		
The Digital Divide		

Tech & The Gender Pay Gap: IT's Complicated

Tech Industry: Male-Dominated at All Levels

■ Men   ■ Women

Job Level	Tech Industry	Non-Tech Industry
Executive	21%	36%
Director	32%	49%
Manager / Supervisor	28%	48%
Individual Contributor	32%	57%
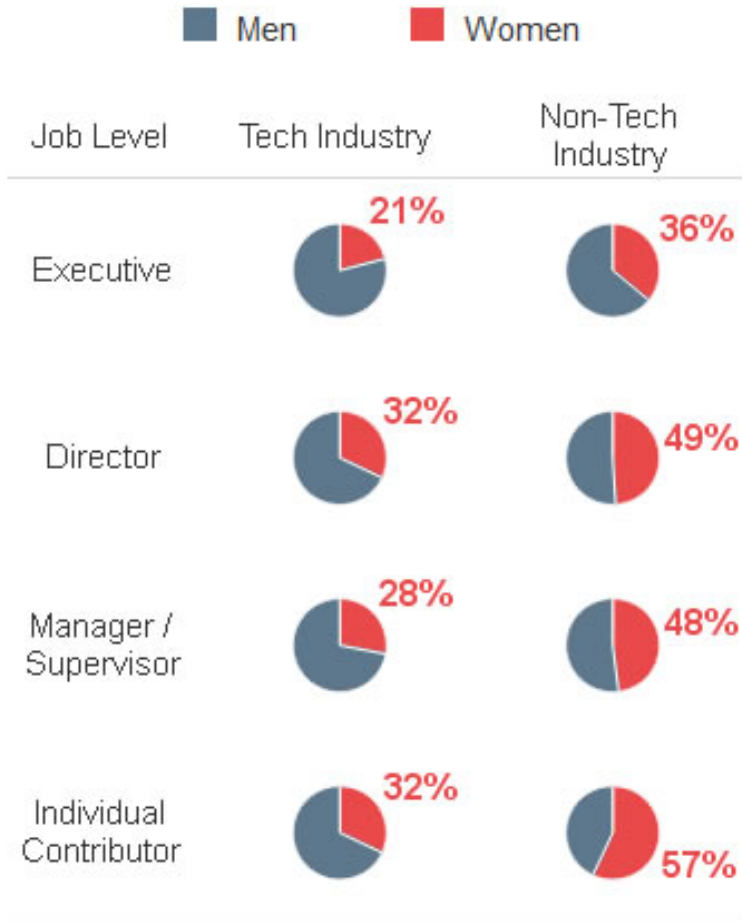
Tech Pays More, But the Gap is Still There

■ Men   ■ Women

Median Pay — Tech Industry / Non-Tech Industry

Tech Industry:
- Individual Contributor: -19%
- Manager / Supervisor: -22%
- Director: -18%
- Executive: -22%

Non-Tech Industry:
- Individual Contributor: -21%
- Manager / Supervisor: -21%
- Director: -20%
- Executive: -32%

$200K
$150K
$100K
$50K
$0K
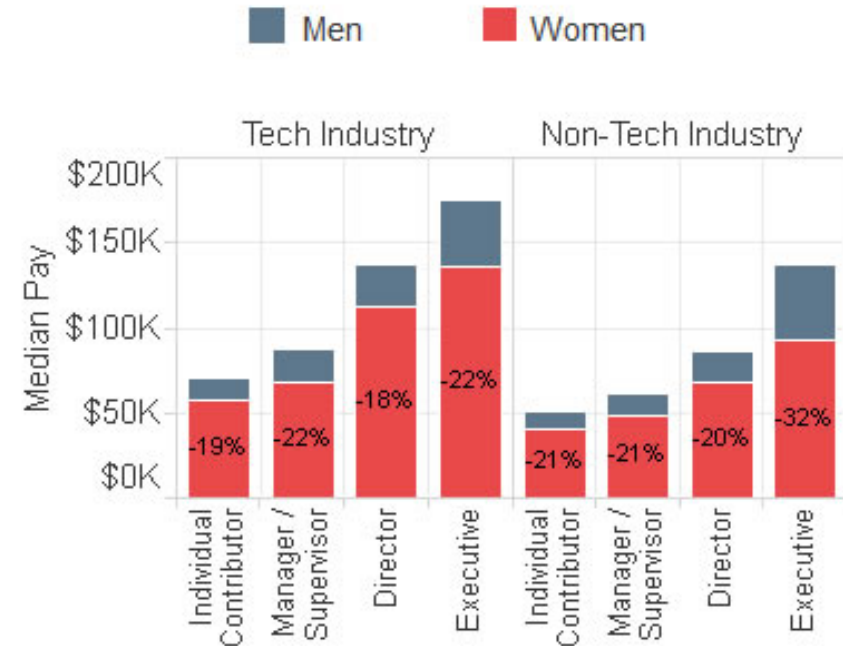
How do you want to compare salaries?
◉ Uncontrolled: All men and all women
○ Controlled: Similar men and women in similar jobs

PayScale

Many companies have begun to implement programs designed to attract more women.

People generally have good intentions, ... but
we all have biases which are invisible to us.

Test yourself: https://implicit.harvard.edu/implicit/
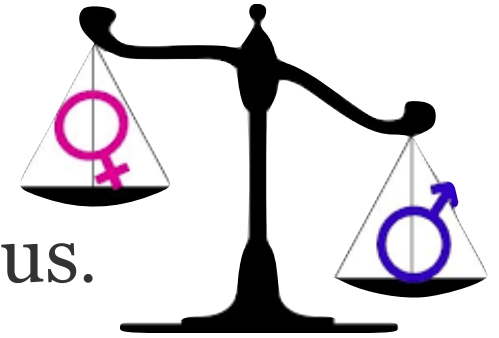
Bias still either keeps women out of the running for promotions or makes women feel left out of the team dynamics.

We want to ensure that our graduates learn to change this.

This starts now.

Changing unconscious gender bias is a process that must be repeated and reinforced on a daily basis.
If you are experiencing gender bias, speak up.
Bring the situation to our attention.

in your interactions with each other

Don't be exclusive

Giving your attention and time to those who look like you in terms of age, gender, race or background reinforces unconscious bias.

Develop a core value system

This value system should focus on fair treatment and respect for others. A basic human right, but one that we can often forget or overlook in the heat and pressure of daily life.

Change your lens

Try using an unconscious bias lens when considering how you interact in teams.

We all are biased to some extent, but consciously becoming aware of it and taking action to address it will benefit us all.

Don't be that person excluding others in the group; recognize your unconscious actions and don't let them hold you or others back.

Making the unconscious conscious will help you make more objective decisions, facilitate inclusive interactions, and create opportunities. Begin unbiasing with education, accountability, measurement, and more.

Google has been on a multi-year journey to understand how decisions are made at work, how inclusive organizational cultures are built and sustained, and how individuals can take conscious control of their actions, behaviors, and cultural contributions. This journey has led Google to dive into the world of the unconscious mind.

Unconscious biases are the automatic, mental shortcuts used to process information and make decisions quickly. At any given moment individuals are flooded with millions of bits of information, but can only consciously process about 40. Cognitive filters and heuristics allow the mind to unconsciously prioritize, generalize, and dismiss large volumes of input. These shortcuts can be useful when making decisions with limited information, focus, or time, but can sometimes lead individuals astray and have unintended consequences in the workplace.

Unconscious bias can prevent individuals from making the most objective decisions. They can cause people to overlook great ideas, undermine individual potential, and create a less than ideal work experience for their colleagues. By understanding unconscious bias and overcoming it at critical moments, individuals can make better decisions - from finding the best talent (no matter what the background) to acknowledging a great idea (no matter who it came from) - and build a workforce and workplace that support and encourages diverse perspectives and contributions.

The scientific evidence demonstrating the negative effects of unconscious bias is well-documented, but there's still a lot to learn about how to mitigate it. Combatting unconscious biases is hard, because their influence on our decisions in a given moment doesn't feel wrong; it feels intuitively right. But in order to create a workplace that supports and encourages diverse perspectives, talents, and ideas, you need to give people the platform and tools to begin unbiasing, Google's term for mitigating unconscious bias and giving your first thoughts a second look. Google is early in the unbiasing journey, but making the unconscious conscious is critical to create a welcoming and inclusive workplace for everyone.

https://rework.withgoogle.com/guides/unbiasing-raise-awareness/steps/introduction/

Privacy, Security, Surveillance and Regulation

Charles D. Raab

Professorial Fellow

School of Social and Political Science

University of Edinburgh

Director of CRISP (Centre for Research into Information, Surveillance and Privacy)

Turing Fellow, Alan Turing Institute

Presented in the Professional Issues Course, School of Informatics, University of Edinburgh, 24 October 2017

© Charles D. Raab 2017

Outline of Lecture

- What is privacy?
- What is security?
- How are they related?
- What is surveillance?
- How does it relate to data science?
- What kinds of regulation?
- Privacy by design and default
- Data science and data
- Internet research
- Ethics, codes, and standards
- Bibliography

Individual Privacy

- Philosophy, social sciences, law: no single definition or conceptualisation
- Seven types (Finn, *et al.,* 2013): privacy of:
  - the person
  - behaviour and action
  - communication
  - data and image
  - thoughts and feelings
  - location and space
  - association
- Other types (Wright and Raab, 2014)
- Context-dependent (Nissenbaum, 2010)
- Conventional privacy paradigm: individualistic, classical liberal, rights-oriented only (Bennett and Raab, 2006)

Individual Privacy's Value

- Deontological (right/wrong action) and consequentialist (right/wrong consequences)
- Privacy is an individual right:
  - fundamental but not absolute (Raab, 2017)
  - 'Everyone has the right to respect for his or her private and family life, home and communications.' (Charter of Fundamental Rights of the EU, Article 7)
  - serves selfhood, autonomy, dignity, but also sociality
- Privacy's importance goes beyond that to the individual; a crucial underpinning of:
  - interpersonal relationships
  - society itself
  - the workings of a democratic political system
- When privacy is protected, the fabric of society, the functioning of political processes and the exercise of important freedoms are protected. When eroded, society and the polity are also harmed; privacy protection is both an individual and a public interest

Privacy and its Social Value (Regan, 1995)

- Common value: all have common interest in right to privacy but may differ on specific content of their privacy or what they think sensitive

- Public value: privacy instrumentally valuable to democratic political system, e.g., for freedom of speech and association, and for setting boundaries to state's exercise of power

- Collective value: economistic conception of privacy's value as collective, non-excludible good that cannot be divided and that cannot be efficiently provided by market

- Many other writers on how privacy works in society and social relations

  (Goffman, many works; Westin, 1967; Altman, 1975; Solove, 2008; Schoeman, 1992; Bygrave, 2002; Goold, 2009; Steeves, 2009; Raab, 2014, 2012; …)

- Society, not just the individual, is better off when privacy exists

- Based on understanding privacy's importance for society, social and political relationships; not only for individual rights or values

But What About Security?

- Whatever 'privacy' means, it is not the only important value in policy-making, and not the only public-interest value

- Security is also a fundamental right: 'Everyone has the right to liberty and security of person. (Charter of Fundamental Rights of the EU, Article 6)

- Security (national and other) seems now to be the over-riding value, facing terrorism, crime, many kinds of adverse event

- Does this inevitably lead to (tendentious) 'privacy v. public interest/ security/etc.' construct?

- What else can be said about the relationship between privacy and security? (discussed later)

But what is 'security'?

Some Definitions of 'Security'

- '[T]he condition (perceived or confirmed) of an individual, a community, an organisation, a societal institution, a state, and their assets (such as goods, infrastructure), to be protected against danger or threats such as criminal activity, terrorism or other deliberate or hostile acts, disasters (natural and man-made).' (adopted by CEN BT/WG 161 on Protection and Security of the Citizen, January 2005; cited in Martí Sempere, 2010: 6)

- '[A] fundamental *good* without which societies cannot prosper.'(Martí Sempere 2010: 2; emphasis in original)

- 'The concept of security has for too long been interpreted narrowly: as security of territory from external aggression, or as protection of national interests in foreign policy or as global security from the threat of a nuclear holocaust. It has been related more to nation-states than to people....Forgotten were the legitimate concerns of ordinary people who sought security in their daily lives. For many of them, security symbolized protection from the threat of disease, hunger, unemployment, crime, social conflict, political repression and environmental hazards...In the final analysis, human security is a child who did not die, a disease that did not spread, a job that was not cut, an ethnic tension that did not explode in violence, a dissident who was not silenced. Human security is not a concern with weapons–it is a concern with human life and dignity. ...Human security is *people-centred.* ' (UNDP, Human Development Report 1994: 22-23)

'Security' in Technical Discourse

- 'Computer security, also known as cyber security or IT security, is the protection of computer systems from the theft and damage to their hardware, software, or information, as well as from disruption or misdirection of the services they provide' (Wikipedia, quoting Gasser 1988, p. 3)
- This refers only to one meaning of 'security'
- This refers only to one source of privacy violation
- Data protection (information privacy) principles include this kind of security: '[Personal data shall be] (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures' (EU General Data Protection Regulation, Article 5(1)(f))

Computer/cyber/IT security can protect privacy, but is only part of the whole story

Computer scientists (and related specialists) should therefore think outside their box to the wider legal and ethical frame of reference for 'security'

Security: Types

- **Information** security: to protect information and information systems from unauthorised access, modification or disruption; computer security

- **Physical** security: to safeguard the physical characteristics and properties of systems, spaces, objects and human beings

- **Political** security: protection of acquired rights, established institutions/structures and recognized policy choices

- **Socio-Economic** security: economic measures to safeguard individuals

- **Cultural** security: to safeguard the permanence of traditional schemas of language, culture, associations, identity and religious practices

- **Environmental** security: to provide safety from environmental dangers caused by natural or human processes

- **Radical uncertainty** security: to provide safety from exceptional and rare violence/ threats not deliberately inflicted by an external or internal agent but can still threaten drastically to degrade the quality of life

- **Human** security: to cope with various threats in the daily lives of people

- **National** security: to protect the integrity of sovereign state territory and assets
(Source: partly drawn from PRISMS FP7 project, Deliverable 2.1: *Preliminary report on current developments and trends regarding technologies for security and privacy*, 28 February 2013: 11-12)

Security: Dimensions and Dilemmas

- As with privacy, many ways of understanding this
  - **Individual** or **personal** security; security of personal **data**
  - **Collective** security at many levels beyond the individual: international, national, local, neighbourhood, social group; security of **systems**
  - **Objective** security: probabilities of risk
  - **Subjective** security: feelings of (in)security
- Which (if any) of these should prevail, and how can they be reconciled?
- 'A man's home is his castle': privacy and liberties/freedoms can be regarded in some respects as valuable because of the security and safety – not least, of personal data – they provide for individuals, groups and societies (cf. *Liberty and Security in a Changing World:* 14; Raab 2014)

  If so, the relationship between privacy and security is far more complex and cannot be glossed over by a rhetoric of the 'opposed' rights or values of security and privacy

Conflict Between Privacy and Security?

- '[t]he realm of rights, private choice, self-interest, and entitlement…[*versus*] corollary social responsibilities and commitments to the common good… [their neglect has] negative consequences such as the deterioration of public safety…' (Etzioni 1999: 195)

But what does this construction ignore?

Does this construction have any practical effect?

Intelligence and Security Committee of Parliament: Call for Evidence (2013)

- 'In addition to considering whether the current statutory framework governing access to private communications remains adequate, the Committee is also considering the appropriate balance between our individual right to privacy and our collective right to security.'

- Rhetorical and imprecise, impeding deeper understanding of what is at stake for the individual, society and the state

- Three difficulties: (Raab, 2017)

> 'privacy'

> 'security'

> 'national security v. personal privacy' framing

Former UK Foreign Secretary's View

Philip Hammond, Intelligence and Security Speech at the Royal United Services Institute, 10 March 2015

'We are after all, all of us in our private lives, <u>individuals</u> who seek privacy for ourselves and our families, as well as <u>citizens</u> who demand protection by our government from those who would harm us. So we are right to question the powers required by our agencies – and particularly by GCHQ – to monitor private communications in order to do their job. But we should not lose sight of the vital balancing act between the <u>privacy we desire</u> and the <u>security we need</u>.' (emphasis added)

Review Group on Intelligence and Communications Technologies
Liberty and Security in a Changing World (12/12/13)

'We suggest careful consideration of the following principles: [pp.14-16]

'1. The United States Government must protect, at once, two different forms of security: national security and personal privacy.

'In the American tradition, the word "security" has had multiple meanings. In contemporary parlance, it often refers to national security or homeland security. One of the government's most fundamental responsibilities is to protect this form of security, broadly understood. At the same time, the idea of security refers to a quite different and equally fundamental value, captured in the Fourth Amendment to the United States Constitution: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . ". Both forms of security must be protected.'

'Balance'?

- Conventional privacy paradigm: 'balancing' as policy aim (but thumb on scale)
- Problems with 'balance' (e.g., Loader and Walker, 2007; Waldron, 2003; Dworkin, 1977; Zedner, 2009; Raab, 1999; RUSI, 2013; Anderson, 2013; others)
- 'The idea of "balancing" has an important element of truth, but it is also inadequate and misleading. It is tempting to suggest that the underlying goal is to achieve the right "balance" between the two forms of security [national security and personal privacy]. …But some safeguards are not subject to balancing at all. In a free society, public officials should never engage in surveillance in order to punish their political enemies; to restrict freedom of speech or religion; to suppress legitimate criticism and dissent; to help their preferred companies or industries; to provide domestic companies with an unfair competitive advantage; or to benefit or burden members of groups defined in terms of religion, ethnicity, race, and gender.' (Review Group on Intelligence and Communications *Technologies, Liberty and Security in a Changing World* (12/12/13))

'(National) Security v. Personal Privacy' ?

- 'How much security should we give up to protect privacy?' is rarely asked

- Assumptions about risk, equilibrium and a common metric for weighing are not clear and doubtfully warranted

- Can we know and agree how much (and whose) privacy should or should not outweigh how much (and whose) security?

- 'Balancing' is silent about the method by which a balance can be determined and challenged, and about who is to determine it

- Whether 'balance' is a noun or a verb, and refers to a method or to its outcome, is often ambiguous; legal case decisions are one source for understanding, and perhaps disputing, the weighing process and the arguments used, for instance about necessity and proportionality

- Remains to be seen how these understandings can be disseminated in the much more closed conditions of the intelligence and security service/law enforcement where strategic and operational decisions have to be made, and also brought to bear in their oversight and scrutiny

PRISMS Project: Selected Survey Findings

- *Both* privacy and security important to people

- People do *not* value security and privacy in terms of 'trade-off'

- No significant relationship between people's valuation of privacy and valuation of security

- Significant correlation between valuation of personal and general security

Security and Privacy: Affinities (Raab, 2014, 2012)

- Privacy *itself* is a security value, often promoted as such

  protective, defensive, precautionary, risk-aversion value

  in face of technologically assisted policy initiatives

  in society driven by counter-terrorism, law-enforcement, preoccupation with personal safety

  provides secure refuge for individuals and groups

  for inward-looking purposes

  for external sociality and participation

  guarding against spatial or informational encroachments

- Privacy advocates (often fear-driven) invoke precautionary principle, criticising state security policies and surveillance technologies

- 'Privacy impact assessment' based on precautionary risk-minimisation

- 'Securitisation' of information or systems in interest of privacy (e.g., encryption)

- Both privacy and security of society or state can therefore be seen as two 'takes' on public interest, changing nature of argument

Surveillance: Types

- watching (eyes and cameras)
- listening (ears and electronic devices)
- locating/tracking
- detecting/sensing
- personal data monitoring ('dataveillance')
- data analytics ('big data')

All have potential or actual impact on ethical and social values, including <u>privacy;</u> but what's that? (see earlier)

All used for purposes of <u>security;</u> but what's that? (see earlier)

All subject to <u>regulation;</u> but how?

From Computer Science to 'Data Science'

- Data science: extracting knowledge or insights from data
- Much of the data are personal data
- Much of the personal data are gathered through surveillance
- Much surveillance uses technologies designed for that purpose
- Much of data science data uses technologies and processes designed for extracting knowledge and insights

Does this require regulation? What and how?

Regulatory Instruments

- Laws and regulatory agencies
- Codes of practice/ethics/standards
- Privacy-enhancing technologies (PETs)
- Privacy by design (and default) (PbD)
- Public awareness
- Training requirements for data users

These instruments relate to the protection of personal data, not to all forms of surveillance if personal data are not 'processed' (collected, stored, etc.)

Privacy/Data Protection by Design and by Default (1)

EU, General Data Protection Regulation (2016)

*Article 25 **Data protection by design and by default***

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

Privacy/Data Protection by Design and by Default (2)

Recital 78

The protection of the rights and freedoms of natural persons with regard to the processing of personal data require that appropriate technical and organisational measures be taken to ensure that the requirements of this Regulation are met. In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. Such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations. The principles of data protection by design and by default should also be taken into consideration in the context of public tenders.

Privacy, Security, and (D)PbD

- *Information* security is also (part of) information privacy, provided through technological means
- Designing-in, and defaulting to, privacy is to provide a **collective** good to be enjoyed by all who use the technology or system, not a good to be chosen as an 'extra' by the individual who happens to care about privacy
- '[M]any technologies and information systems exacerbate social differences….This social division is likely to happen unless privacy's collective value is explicitly recognized in organizational practice and built into the construction of information and communications technologies and systems. However, this value could be subverted if some people were better able than others to buy protective information technologies for their own use, in keeping with the individualist paradigm. This would be the information society's equivalent of "gated communities".' (Bennett and Raab, 2006: 41-2)
- This further underlines the **affinity between privacy and security**, whether individual or collective
- It brings *equality* into view as a neglected dimension of these debates

Ethical Robotics?: BS 8611: 2016

- 'This British Standard gives guidance on the identification of potential ethical harm and provides guidelines on safe design, protective measures and information for the design and application of robots'

- 'Ethical hazards are broader than physical hazards. Most physical hazards have associated psychological hazards due to fear and stress. Thus, physical hazards imply ethical hazards and safety design features are part of ethical design. Safety elements are covered by safety standards; this British Standard is concerned with ethical elements'

- 'Examples of ethical harm include stress, embarrassment, anxiety, addiction, discomfort, deception, humiliation, being disregarded. This might be experienced in relation to a person's gender, race, religion, age, disability, poverty or many other factors'

'Facebook reveals news feed experiment to control emotions'

'Protests over secret study involving 689,000 users in which friends' postings were moved to influence moods' (Robert Booth, *The Guardian*, Monday, 30 June 2014)

'In a study with academics from Cornell and the University of California, Facebook filtered users' news feeds – the flow of comments, videos, pictures and web links posted by other people in their social network. One test reduced users' exposure to their friends' "positive emotional content", resulting in fewer positive posts of their own. Another test reduced exposure to "negative emotional content" and the opposite happened.

'James Grimmelmann, professor of law at Maryland University, said Facebook had failed to gain "informed consent" as defined by the US federal policy for the protection of human subjects, which demands explanation of the purposes of the research and the expected duration of the subject's participation, a description of any reasonably foreseeable risks and a statement that participation is voluntary. "This study is a scandal because it brought Facebook's troubling practices into a realm – academia – where we still have standards of treating people with dignity and serving the common good," he said.'

Dataveillance: Profiling

Analysis of data on (e.g.) drug use, crime, migrants, asylum-seekers, welfare fraud, consumption history, internet behaviour, credit history, education records, health, etc.

Potentially beneficial, potentially harmful, for individuals or society

Identifies or creates groups, categories, individuals

Predicts behaviour

Decisions based on profiles

False positives, false negatives

'Social sorting': discrimination, social exclusion/inclusion

Used by states/public authorities, law enforcers, businesses; researchers

Internet Research: What is it? (1)

'This document uses the following working definitions:

Internet research encompasses inquiry that:

(a) utilizes the internet to collect data or information, e.g., through online interviews, surveys, archiving, or automated means of data scraping;

(b) studies how people use and access the internet, e.g., through collecting and observing activities or participating on social network sites, listservs, web sites, blogs, games, virtual worlds, or other online environments or contexts;

(c) utilizes or engages in data processing, analysis, or storage of datasets, databanks, and/or repositories available via the [internet]

(d) studies software, code, and internet technologies

(e) examines the design or structures of systems, interfaces, pages, and elements

(f) employs visual and textual analysis, semiotic analysis, content analysis, or other methods of analysis to study the web and/or internet-facilitated images, writings, and media forms.

(g) studies large scale production, use, and regulation of the internet by governments, industries, corporations, and military forces.'

Internet Research: What is it ? (2)

'The internet is a social phenomenon, a tool, and also a (field) site for research. Depending on the role the internet plays in the research project or how it is conceptualized by the researcher, different epistemological, logistical and ethical considerations will come into play. The term "Internet" originally described a network of computers that made possible the decentralized transmission of information. Now, the term serves as an umbrella for innumerable technologies, devices, capacities, uses, and social spaces. Within these technologies, many ethical and methodological issues arise and as such, internet research calls for new models of ethical evaluation and consideration. Because the types of interaction and information transmission made possible by the internet vary so widely, researchers find it necessary to define the concept more narrowly within individual studies. This is complicated by the fact that studies of and on the internet cut across all academic disciplines.'

Final Copy: Ethical Decision-Making and Internet Research: Recommendations from the AOIR Ethics Committee. Approved by the Ethics Working Committee, 08/2012. Endorsed by the AOIR Executive Committee, 09/2012. Approved by the AOIR general membership, 12/2012.

Internet Research Ethics (IRE) (1)

'*IRE* is defined as the analysis of ethical issues and application of research ethics principles as they pertain to research conducted on and in the Internet. Internet-based research, broadly defined, is research which utilizes the Internet to collect information through an online tool, such as an online survey; studies about how people use the Internet, e.g., through collecting data and/or examining activities in or on any online environments; and/or, uses of online datasets, databases, or repositories.'

Ess, Charles and the Association of Internet Researchers Ethics Working committee, 2002, "Ethical Decision-Making and Internet Research: Recommendations from the AoIR Ethics Working Committee," quoted in 'Internet Research Ethics', *Stanford Encyclopedia of Philosophy*, 2012

Internet Research Ethics (IRE) (2)

'The multiple disciplines already long engaged in human subjects research (medicine, sociology, anthropology, psychology, communication) have established ethical guidelines intended to assist researchers and those charged with ensuring that research on human subjects follows both legal requirements and ethical practices. But with research involving the Internet—where individuals increasingly share personal information on platforms with porous and shifting boundaries, where both the spread and aggregation of data from disparate sources is increasingly the norm, and where web-based services, and their privacy policies and terms of service statements, morph and evolve rapidly—the ethical frameworks and assumptions traditionally used by researchers and REBs are frequently challenged.'

Stanford Encyclopedia of Philosophy, 2012

Article 29 Data Protection Working Party: WP203 (Opinion 03/2013 on Purpose Limitation)

'Under the current framework [EU Data Protection Directive 95/46/EC], it is up to each Member State to specify what safeguards may be considered as appropriate. This specification is typically provided in legislation, which could be precise (e.g. national census or other official statistics) or more general (most other kinds of statistics or research). In the latter case, this leaves room for professional codes of conduct and/or further guidance released by the competent data protection authorities.'

Codes, Statements, Etc.: Mainly General

BSA (British Sociological Association) 2002

ASA (American Sociological Association) 1999/2008

BPS (British Psychological Society) 2013

PSA (Political Studies Association) n.d. (1990s)

SRA (Social Research Association) 2003

AAAS (American Association for the Advancement of Science) 2014

MRS (Market Research Society) 2014

AOIR (Association of Internet Researchers) 2002/2012

UKRIO (UK Research Integrity Office) 2009 [adopted by the University of Edinburgh]

etc.

UKRIO: Code of Practice for Research (2009)

High-level template

No mention of privacy (does mention personal data)

No mention of Internet

No mention of social media

   But…

'3.7.1 Organisations and researchers should make sure that any research involving human participants, human material or personal data complies with all legal and ethical requirements and other applicable guidelines. Appropriate care should be taken when research projects involve: vulnerable groups, such as the very old, children or those with mental illness; and covert studies or other forms of research which do not involve full disclosure to participants. The dignity, rights, safety and well-being of participants must be the primary consideration in any research study. Research should be initiated and continued only if the anticipated benefits justify the risks involved.'

UKRIO: Code of Practice for Research (2009)

'3.7.3 Organisations and researchers should ensure the confidentiality and security of: personal data relating to human participants in research; and human material involved in research projects.'

'3.7.10 Researchers on projects involving human subjects must satisfy themselves that participants are enabled, by the provision of adequate accurate information in an

appropriate form through suitable procedures, to give informed consent, having particular regard to the needs and capacities of vulnerable groups, such as the very old, children and those with mental illness.'

University of Edinburgh College of Humanities and Social Science Research Ethics Framework, May 2008

- High-level principles

- Mentions dignity

- Mentions consent

- 'The storage, processing and disposal of information about individuals who are research subjects must meet legal requirements, including the individual's explicit written consent to the proposed holding and use of the data. Individuals' right to access and correct information held about them should also be explained.'

   but 'explicit __written__ consent' is not part of the UK Data Protection Act 1998, Schedule 3, even for processing 'sensitive' personal data; nor is it part of the EU General Data Protection Regulation

However...

'But as online research takes place in a range of new venues (email, chatrooms, webpages, various forms of "instant messaging," MUDs and MOOs, USENET newsgroups, audio/video exchanges, etc.) – researchers, research subjects, and those charged with research oversight will often encounter ethical questions and dilemmas that are not directly addressed in extant statements and guidelines. In addition, both the great variety of human inter/actions observable online and the clear need to study these inter/actions in interdisciplinary ways have thus engaged researchers and scholars in disciplines beyond those traditionally involved in human subjects research: for example, researching the multiple uses of texts and graphics images in diverse Internet venues often benefits from approaches drawn from art history, literary studies, etc. This interdisciplinary approach to research leads, however, to a central ethical difficulty: the primary assumptions and guiding metaphors and analogies - and thus the resulting ethical codes - can vary sharply from discipline to discipline, especially as we shift from the social sciences (which tend to rely on medical models and law for human subjects' protections) to the humanities (which stress the agency and publicity of persons as artists and authors).'

Charles Ess and the AoIR ethics working committee, 'Ethical decision-making and Internet research: Recommendations from the AoIR ethics working committee', Approved by AoIR, November 27, 2002, www.aoir.org/reports/ethics.pdf

Therefore…

- Need to review and revise ethical and legal principles, codes and guidance for research using 'big data'/analytics; is this happening?

- Need to recognise that, especially where principles, codes and guidelines leave off, **judgement** must be exercised because conflicting rights and interests are involved; no 'tick-boxes'

- Judgement is needed about the justification of 'big data' research; its limits; its (un)intended consequences; its risks; its legality; its ethics

(How) can researchers be trained to exercise judgement of this kind?

Bibliography (1)

- Altman, I. (1975), *The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding*, Monterey, CA: Brooks/Cole Publishing Co.

- Anderson, D. (2015), *A Question of Trust: Report of the Investigatory Powers Review* [Anderson Report], London: The Stationery Office.

- Bauman, Z. (2006), *Liquid Fear*, Cambridge: Polity Press.

- Bennett, C. and Raab, C. (2006), *The Governance of Privacy: Policy Instruments in Global Perspective*, Cambridge, MA: The MIT Press.

- Bygrave, L. (2002), *Data Protection Law: Approaching its Rationale, Logic and Limits,* The Hague: Kluwer Law International.

- Dworkin, R. (1977), *Taking Rights* Seriously, London: Duckworth.

- Etzioni, A. (1999), *The Limits of Privacy*, New York, NY: Basic Books.

- European Union (2016), *General Data Protection Regulation*

- Finn, R., Wright, D. and Friedewald, M. (2013), 'Seven Types of Privacy', pp. 3-32 in S. Gutwirth, R. Leenes, P. De Hert, et al. (eds.), European Data Protection: Coming of Age?, Springer.

Bibliography (2)

- Gasser, M. (1988) *Building a Secure Computer System*, Van Nostrand Reinhold

- Goffman, E. (many works)

- Goold, B. (2009), 'Surveillance and the Political Value of Privacy'. *Amsterdam Law Forum* 1(4). http://amsterdamlawforum.org.

- Intelligence and Security Committee of Parliament (2015), *Privacy and Security: A Modern and Transparent Legal Framework*, London: The Stationery Office.

- Loader, I. and Walker, N. (2007), *Civilizing Security*, Cambridge: Cambridge University Press.

- Martí Sempere, C. (2010). "The European Security Industry: A Research Agenda". Economics of Security Working Paper 29, Berlin: Economics of Security.

- Nissenbaum, H. (2010), *Privacy in Context. Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford University Press.

- Raab, C. (1999),'From Balancing to Steering: New Directions for Data Protection', pp. 68-93 in C. Bennett and R. Grant (eds.), *Visions of Privacy: Policy Approaches for the Digital Age*, Toronto: University of Toronto Press.

- Raab, C. (2012), 'Privacy, Social Values and the Public Interest', pp. 129-151 in A. Busch and J. Hofmann (eds.) 'Politik und die Regulierung von Information' ['Politics and the Regulation of Information'], *Politische Vierteljahresschrift* Sonderheft 46, Baden-Baden: Nomos Verlagsgesellschaft.

Bibliography (3)

- Raab, C. (2014), 'Privacy as a Security Value', pp. 39-58 in D. W. Schartum, L. Bygrave and A. G. B. Bekken (eds.), *Jon Bing: En Hyllest / A Tribute*, Oslo: Gyldendal; available at: http://bigdataandprivacy.org/wpcontent/uploads/2014/08/Raab_PrivacySecurityValue.pdf

- Raab, C. (2017)*, 'Security, Privacy and Oversight', pp. 77-102 in Andrew Neal (ed.), *Security in a Small Nation: Scotland, Democracy, Politics*. Cambridge: Open Book Publishers.

- Regan, P. (1995*), Legislating Privacy: Technology, Social Values, and Public Policy*, Chapel Hill, NC: University of North Carolina Press.
Review Group on Intelligence and Communications (2013) *Technologies, Liberty and Security in a Changing World*, Washington, DC.

- Royal United Service Institute for Defence and Security Studies (2015), *A Democratic Licence to Operate: Report of the Independent Surveillance Review*, London: Royal United Services Institute for Defence and Security Studies.

- Schoeman, F. (1992), *Privacy and Social Freedom* Cambridge: Cambridge University Press.

- Solove, D. (2008), *Understanding Privacy*, Cambridge, MA: Harvard University Press.

- Steeves, V. (2009), 'Reclaiming the Social Value of Privacy', pp. 191-208 in I. Kerr, V. Steeves and C. Lucock (eds.), *Lessons From the Identity Trail: Privacy, Anonymity and Identity in a Networked* Society, Oxford: Oxford University Press

Bibliography (4)

- The President's Review Group on Intelligence and Communications Technologies (2013) *Liberty and Security in a Changing* World – *Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies*, December 12, 2013 (Washington, DC).

- United Nations Development Programme (1994), *Human Development Report 1994*, New York, NY: Oxford University Press.

- Waldron, J. (2003), 'Security and Liberty: The Image of Balance', *The Journal of Political Philosophy*, vol. 11, pp. 191-210.

- Westin, A. (1967), *Privacy and Freedom*. New York, NY: Atheneum.

- Wright, D. and Raab, C. (2014), 'Privacy Principles, Risks and Harms', *International Review of Law, Computers & Technology*, Vol. 28, No. 3, pp. 277-298.

- Zedner, L. (2009), *Security,* London: Routledge.

c.d.raab@ed.ac.uk

General Data Protection Regulation

Based on the Pinsent Mason Paper

New Features of the GDPR

- Accountability measures: GDPR requires compliance and *evidence* of compliance:
  - documented policies and procedures,
  - records of consents etc.
  - Registration with supervisory authorities (e.g. ICO) no longer required.
    - internal record-keeping obligations
    - supervisory authorities can demand information, conduct audits, order remediation etc.
- Territorial scope (Article 3)
  - extending to non-EU controllers and processors in some cases.
  - "one stop shop": organisations operating in multiple EU Member States report to only one main supervisory authority.
  - Consistency mechanism to promote harmonisation across EU Member States and resolve cross-border issues.

New Features of the GDPR

- Amended definitions (Article 4), e.g.
  - expanded definitions of "personal data" and "data subject" (catching more types of data and processing operations)
  - new definitions e.g. "pseudonymisation" and "profiling".
  - Consent will be more difficult to use as a legal basis.
- Direct statutory obligations (Articles 28, 30, 44-49, 33(2)) and liability (Article 82) on processors, and additional requirements regarding the minimum terms that must be included in personal data processing contracts (Article 28).
- Tighter rules on international transfers, applicable to both controllers and processors.

New Features of the GDPR

- Requirement for data protection impact assessments before initiating certain types of processing or other processing operations likely to result in a high risk to individuals:
  - must consider at least the issues specified by the Regulation (Article 35)
  - consultation with the supervisory authority required in some circumstances (Article 36).
- Controllers and processors required to appoint a data protection officer in certain circumstances (Articles 37-39).
- Mechanisms for the purposes of demonstrating compliance with the Regulation, involving codes of conduct (Articles 40-41) or certifications (Articles 42-43) approved under the Regulation for these purposes.

New Features of the GDPR

- Responses to a subject access request will have to be provided within a tighter timescale and free of charge (Article 12).
- New data subject rights:
  - "right to be forgotten" or right to erasure (Article 17),
  - "data portability" (Article 20).
- Security breach notification:
  - mandatory "personal data breach" notifications to the supervisory authority without undue delay (within 72 hours where feasible) (Article 33)
  - personal data breach notifications to the data subject without undue delay where there is a high risk to their privacy (Article 34).

New Features of the GDPR

- The introduction of the Board (Section 3 - Articles 68-76) to replace the Article 29 Working Party, with an enhanced role and powers.

- Harsher sanctions and a new framework for fines (in two tiers), which will be substantially higher than under the DPA(Article 83).
  - DPA: the maximum fine is £500,000,
  - GDPR: two tiers of administrative fines levied by supervisory authorities:
    - up to 20 million EUR or 4% of total worldwide turnover if higher
    - up to 10 million EUR or 2% of total worldwide turnover if higher.

DPA Principles in the GDPR

DPA (1998)

1. Personal data shall be processed **fairly and lawfully** and, in particular, shall not be processed unless: (a) at least one of the conditions in Schedule 2 is met, and (b) in the case of sensitive personal data, at Least one of the conditions in Schedule 3 is also met.

2. Personal data shall be obtained only for one or more **specified and lawful purposes**, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be **adequate, relevant and not excessive** in relation to the purpose or purposes for which they are processed.

GDPR

1. Personal data must be:

a)   processed **lawfully, fairly and in a transparent** manner in relation to the data subject ("Lawfullness, fairness and transparency").

b)   collected for **specified, explicit and legitimate** purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ("purpose limitation")

c)   **adequate, relevant and limited** to what is necessary in relation to the purposes for which they are processed ("data minimisation").

DPA Principles in the GDPR

DPA (1998)

4. Personal data shall be **accurate and, where necessary, kept up to date**.

5. Personal data processed for any purpose or purposes shall **not be kept for longer than is necessary** for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

GDPR

d) **accurate and, where necessary, kept up to date**; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are **erased or rectified without delay** ("accuracy").

e) kept in a form which permits identification of data subjects for **no longer than is necessary for** the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ("storage limitation").

DPA Principles in the GDPR

7. Appropriate technical and organisational measures shall betaken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate LeveE of protection for the rights and freedoms of data subjects in relation to the processing of personaL data.

f) processed in a manner that **ensures appropriate security** of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or dam age, using **appropriate technical or organisational measures** ("integrity and confidentiality").

No equivalent principle, although the area of transferring personal data to a third country or international organisation is dealt with at length in the GDPR.

2. The controller shall be **responsible for and be able to demonstrate compliance with** paragraph 1 ("accountabiLity").

Professional Issues

Data Protection

(Bott, Ch 13)

Overview

- Overview of the 1998 Data Protection Act (DPA)
  - Definitions
  - Changes since 1984 Act
  - Sensitive Personal Data & Consent
  - The eight principles
- Freedom of Information Act 2000 (FOI)
  - Who it affects
  - Public Rights
  - Publication Schemes
  - Exemptions
  - Key Points
- Computer Misuse
- Here we focus on the DPA – we will mention FoI and Misuse in later lectures.

Motivation for the DPA

- To protect individuals from:
  - The use of inaccurate, incomplete or irrelevant personal information
  - The use of personal information by unauthorized people
  - The use of personal information for purposes other than the purpose for which it was gathered
  - Also some sensitivity to transborder data flows and the need to avoid data havens in unregulated jurisdictions
- Rough timeline:
  - Concerns surface in the 1970's (Lindop report more or less says "free text systems should not be used").
  - First act in 1984 – protect people from misuse of data by organisations
  - European directive on Data Protection 1995 – protection from misuse of data on the Internet)
  - Revised act repeals the first act in 1998 – balancing freedom to process against personal privacy

Definitions

- **Data**: information in electronic or manual form
- **Data subject**: individual who is the subject of the personal data
- **Personal Data**: Expression of opinion, or fact, E-mail address, photos, video footage... New category of *sensitive data (e.g. ethnic origin, trade union memership)*.
- **Data Controller**: determines why or how personal data is processed
- **Data Processor**: anyone processing data for the data controller who is not an employee of the data controller
- **Processing**: Reviewing, holding, sorting, deleting, correlating, modifying, ...
- **Relevant Filing System**: Readily accessible information about living individuals
- **Information Commissioner**: New name for Data Protection Registrar

New Provisions in the 1998 Act

- Broader than the old act to comply with European requirements and new threats.

- Strengthened rights for data subjects.

- Extended to cover manual filing systems.

- Sensitive data is a new category and has stronger processing requirements.

- Rules about export of data to non-EEA countries.

Principles of the act – 1.

- Non-sensitive Personal data must be processed *fairly* and *lawfully* and shall not be processed unless one of the below is met (schedule 2).
    - Consent – *most important*
    - Contract
    - Legal Obligation
    - Vital interests of subject (life or death!)
    - Public functions
    - Balance of interest

Sensitive Personal Data

- Racial or ethnic origin
- Political opinions
- Religious/similar beliefs
- Trade Union Membership
- Health
- Sexual Life
- Offences

Sensitive Personal Data

- May only be held if one of the below is met:
    - Explicit and *informed* consent
    - Employment Law
    - Vital Interests of Subject
    - Legal Proceedings
    - Medical Purposes (by medical professionals)
    - Equal opportunities monitoring

Consent

- "Freely given specific and *informed* indication of wishes by which the data suject signifies agreement to personal data relating to him/her being processed."

- Can't use implied consent – must get forms back.

- Can't use blanket consent as condition of entry.

Fair processing

- Must not intentionally or otherwise deceive or mislead subject as to purpose of data use/ collection.

- Must identify to subject data controller/ nominated representative.

- Must identify to subject purpose of processing data.

- Exceptions are disproportionate effort (direct marketing not allowed) or legal obligation.

DPA Principle 2

- Data must be obtained only for one or more specified lawful purposes and shall not be further processed in any manner incompatible with that purpose or purposes.
  - Must not use data for a new incompatible purpose without subject's consent.
  - Have a data protection statement that explains why data will be held and requesting consent in the case of sensitive personal data.
  - The Information Commissioner must be notified by Data Controllers specifying what data will be collected and for what purpose.

DPA Principles 3 & 4

- Personal data must be adequate, relevant and not excessive in relation to the purpose or purposes for which they are to be processed.
  - Volume and type of data can only be justified in relation to the purposes registered with the Information Commissioner
- Personal data shall be accurate and, where necessary, kept up to date.
  - Data holdings must be under continuous review and policies need to be in place to delete old data. Issues about things like addresses for students.

DPA Principle 5

- Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or purposes.

  – Establish how long data needs to be retained. Some needs to be retained forever. (Should School Qualifications be retained forever?)

  – Ensure that such data is really erased (e.g. from dumps, backups, …).

DPA Principle 6

- Personal data must be processed in accordance with the rights of data subjects
  - This means that you cannot do things that violate the rights given to data subjects under the new act, especially denying access to data.

Rights of data subjects

- Must be informed if personal data are being processed and given a description of the personal data
- Be informed of the purpose for which data is being held and processed
- Must be informed of people or organisations to whom personal data might be disclosed
- Be provided with an intelligible description of the specific data held about them
- Be provided with a description of the source of personal data
- May prevent processing for purposes of direct marketing
- May prevent processing likely to cause damage and distress
- Right to compensation in the case of damage caused by processing of personal data in violation of the act.
- Right to see the methods used to score the individual used by credit scoring agencies.

Access rights

- Right to have communicated to him/her in an intelligible form the information constituting the data.

- No right to rifle through filing systems, computers etc.

- Right to be informed of logic involved in automated processing.

- Request must be in writing, fee up to £10 may be charged and identity may be thoroughly checked.

Access rights

- Data may be witheld if disclosure would disclose data about a third party unless:

  – Third party has consented to disclosure

  – It is reasonable to comply without the third party's consent.

  – Duty of confidentiality, steps taken to seek consent, express refusal of third party.

  – Witnesses, confidential reports, access to references.

Access rights

- Don't have to disclose references you have written but must disclose those you have received unless the writer explicitly asked them to kept confidential.
- 40 days to comply (or state reason for refusal to comply) with requests.
- Don't need to comply with repeat requests until a reasonable amount of time has elapsed.
- Don't need to comply if disproportionate effort would be involved.
- Subject must provide reasonable data you request to assist in finding the data.

Enforced Access

- It is an offence to force subjects to exercise their access rights to data held by others
  - Includes data about cautions, criminal convictions and certain social security records

Right to prevent processing

- Unwarranted substantial damage or distress to subject.

- 21 days to comply with request.

- Exemption if processing is necessary for performance of contract with subject or there is a legal obligation, or the vital interests of the subject are at stake.

Exemptions to access rights

- Prevention and detection of crime
- Apprehension or prosecution of offenders
- Collection of tax or other duty
- Research, history, statistics.
- Exam marks – 40 days after date of announcement or 5 months of access request.
- Confidential references.

DPA Principle 7

- Appropriate technical or organisational measures shall be taken against unauthorised or unlawful processing of data and against accidental loss, damage or destruction of personal data.
  - Careful selection of IT staff
  - Appropriate backup policies
  - Use of passwords, encryption etc
  - Use of integrity checking

DPA Principle 8

- Personal data shall not be transferred to a country or territory outside the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

  – Websites are problematic in terms of jurisdiction.

Notifying the Information Commissioner

- Each legal entity intending to hold or process personal data must register with the Information Commissioner.

- The register is public.

- Penalties for failure to comply are substantial.

- The Information Commissioner has strong powers of search and seizure if violations of the DPA are suspected.

Exercise

- Get into a group of two people.
- Look at the entries in the Data Protection Register:
  - https://ico.org.uk/ESDWebPages/Entry/ZA036088
  - https://ico.org.uk/ESDWebPages/Entry/Z5939707
- Do the following:
  - Individually, look at the section on the use of video data – are there any of the DPA principles you feel might be violated by the use of such data. Make a list of the top three.
  - Get together with the other group member and combine your list to create a joint top three principles you feel might be violated. List what principle they violate and how you think a violation could arise.
  - Choose one of the principles and suggest changes that could make the use of video data more compliant with that principle.

The GDPR and Its Implications On Cloud Services

September 2017

Norm Barber, Managing Director
(normb@unifycloud.com)

UnifyCloud

UnifyCloud LLC – General Background

A rapidly growing and successful Redmond, WA-based solutions developer with significant technical resources located in the US and India. Our global focus is on **Cloud**, **Cybersecurity**, **Compliance** (regulatory) and **Cost**.

Effectively migrating from a traditional, on-premises IT environment to a Hybrid IT environment that may include elements of SaaS, IaaS, and PaaS requires a logical set of steps.

As Gartner has noted, "An organization cannot simply 'jump' to the Cloud. **There need to be activities that are part of a phased evaluation and plan to move to the Cloud.**"

| Discover | Assess | Target | Migrate | Monitor |

← The General Data Protection Regulation (GDPR) impacts the entire Cloud (SaaS, IaaS, PaaS) journey →

Disclaimer

This presentation is a commentary on the GDPR, as UnifyCloud LLC interprets it, as of the date of publication. We've spent a lot of time with GDPR and like to think we've been thoughtful about its intent and meaning. But the application of GDPR is highly fact-specific, and not all aspects and interpretations of GDPR are well-settled.

As a result, this presentation is provided for informational purposes only and should not be relied upon as legal advice or to determine how GDPR might apply to you and your organization. We encourage you to work with a legally qualified professional to discuss GDPR, how it applies specifically to your organization, and how best to ensure compliance.

UNIFYCLOUD LLC MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS WHITE PAPER. This presentation is provided "as-is." information and views expressed in this presentation, including URL and other Internet website references, may change without notice.

UnifyCloud

Today's GDPR briefing topics

- What is the GDPR

- How to interpret the GDPR

- Addressing GDPR compliance in the Cloud

- GDPR Baseline approach

- Case Study: Managing GDPR in Azure

UnifyCloud

Audience poll: GDPR key roles that will impact you

Controller (from GDPR)

"…the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law."

Processer (from GDPR)

"… a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller."

Solution Purveyor

- CSV
- ISV
- Consultant

UnifyCloud

Poll:
How ready are you?

UnifyCloud

GDPR key drivers for May 25, 2018 enforcement (in effect as of 5/4/16)

European data protection for the digital era

Better protection for personal data

- Clear consent required to process data
- Limits on the use of automated processing of data to make decisions, for example in the case of 'profiling'
- Right to rectify and remove data, including the 'right to be forgotten' for data collected as a child
- More and clearer information about processing
- Right to move data from one service provider to another
- Easier access to personal data
- Right to notification if data is compromised
- Stricter safeguards for transfers of personal data outside the EU

More opportunities for business

- Level playing field for all EU and non-EU businesses offering goods and services to persons in the EU
- One set of rules for the whole EU
- Rules that allow businesses, especially SMEs, to get the most out of the Digital Single Market
- Risk-based approach, matching obligations of controllers to the level of risk of the processing

More consistent application and effective enforcement

- Individuals and businesses can have their cases dealt with by a data protection authority and a court close to them
- A one-stop shop for individuals and businesses in cross-border cases thanks to the cooperation of national data protection authorities

Fines: up to €20 million OR 4% of global annual turnover

- Updates and modernizes the principles of the 1995 Data Protection Directive

- Sets out the rights of the individual and establishes the obligations of those processing and those responsible for the processing of the data.

- Establishes the methods for ensuring compliance as well as the scope of sanctions for those in breach of the rules.

- Applies to all organizations doing business in the EU regardless of location.

UnifyCloud

GDPR data definitions regardless of nationality or EU residence

Personal Data (from GDPR)

"…means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

Examples:

- Name

- Identification number (e.g., SSN)

- Location data (e.g., home address)

- Online identifier (e.g., e-mail address, screen names, IP address, device IDs)

- Genetic data (e.g., biological samples from an individual)

- Biometric data (e.g., fingerprints, facial recognition)

"The GDPR also requires compliance from non-EU organizations that offer goods or services to EU residents or monitor the behavior of EU residents."

Source: *Brief: You Need An Action Plan For The GDPR*; Forrester Research; October 2016

UnifyCloud

GDPR compliance is a challenge for both controllers and processors

"By the end of 2018, over 50% of companies affected by the GDPR will not be in full compliance with its requirements."

Gartner - *Focus on Five High-Priority Changes to Tackle the EU GDPR*; September 30, 2016

The General Data Protection Regulation (GDPR) imposes new rules on organizations that offer goods and services to people in the European Union (EU), or that collect and analyze data tied to EU residents, no matter where they are located.

- **Enhanced** personal privacy rights

- **Increased** duty for protecting data

- **Mandatory** breach reporting

- **Significant** penalties for non-compliance

UnifyCloud
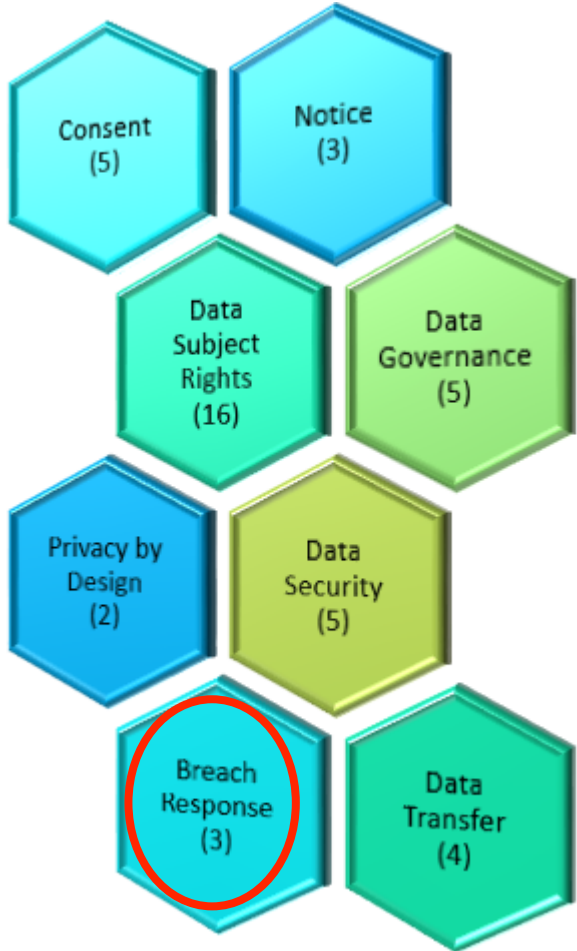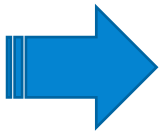
Controller's (or your customer's) GDPR compliance model

43 GDPR Requirements*

GDPR Regulation (261 pages)

Consent (5)

Notice (3)

Data Subject Rights (16)

Data Governance (5)

Privacy by Design (2)

Data Security (5)

Breach Response (3)

Data Transfer (4)
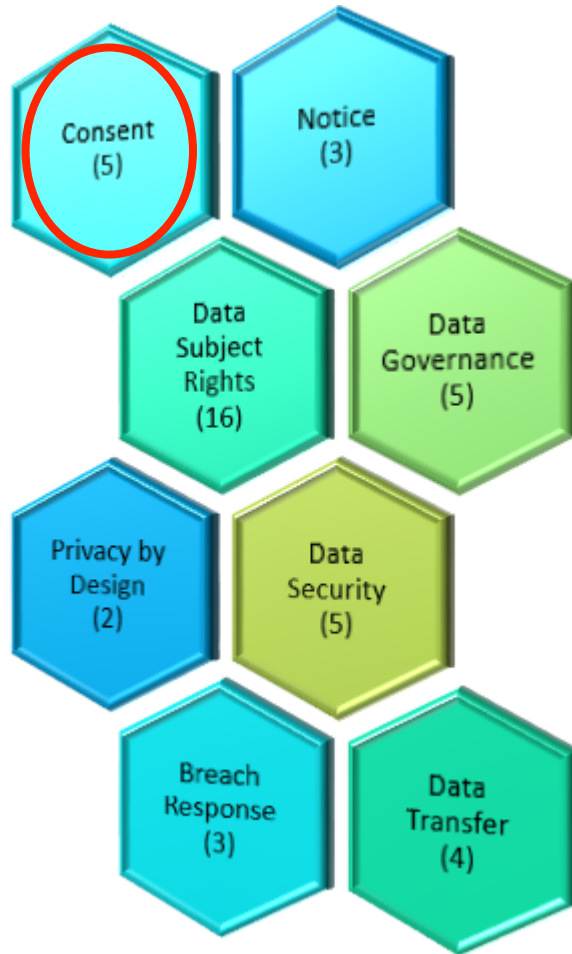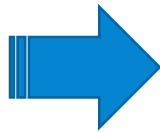
1. Provide notification to data subjects, in clear and plain language.

2. Request and obtain the data subject's affirmative and granular consent.

3. Discontinue with processing activities if the data subject denies consent.

4. Provide a mechanism for data subjects to withdraw consent.

5. Obtain affirmative consent from a child's (under age of 16) parent or guardian.

"…organizations must demonstrate that they have implemented appropriate measures to mitigate privacy risks. Even in the absence of a privacy breach or customer complaint, regulators may require firms to exhibit evidence of their compliance and risk management strategies, including a privacy impact assessment (PIA) when appropriate."

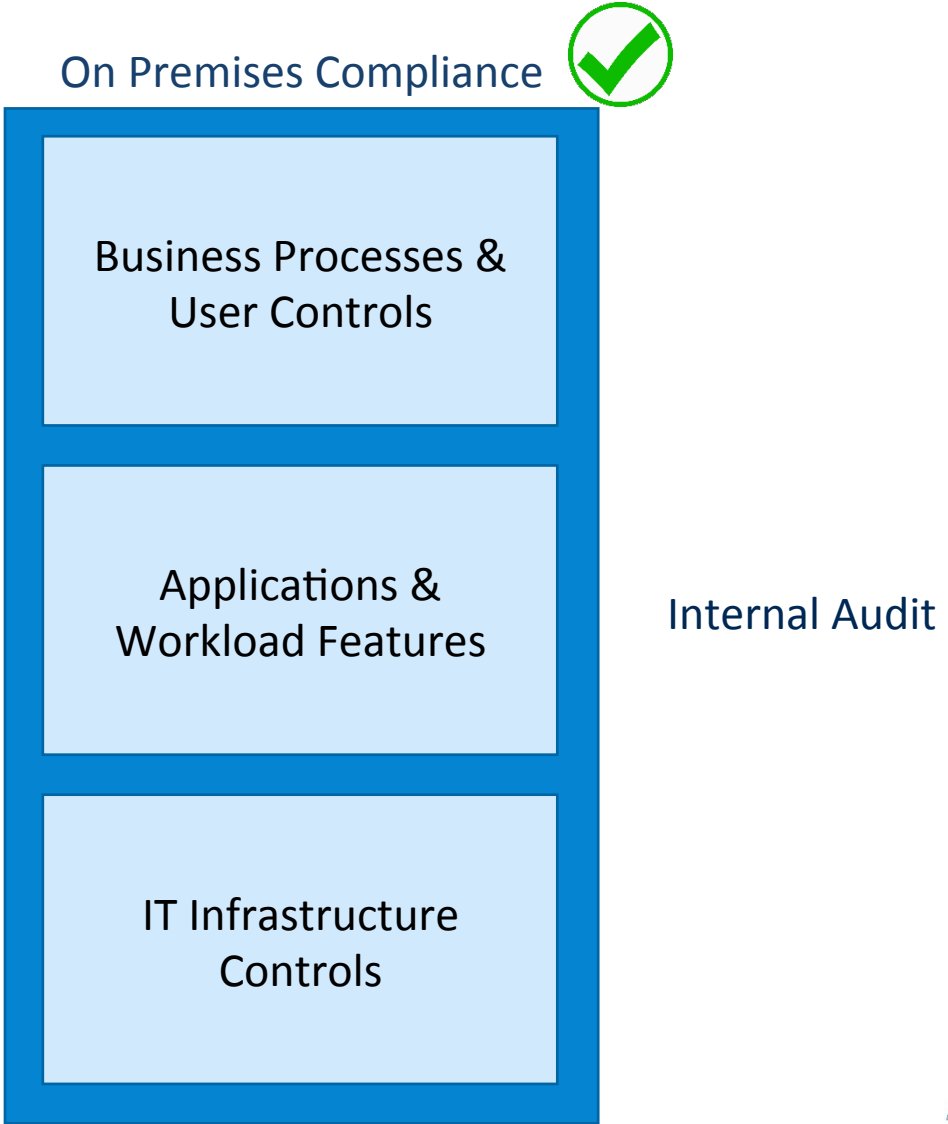**Source**: *Brief: You Need An Action Plan For The GDPR*; Forrester Research; October 2016

* UnifyCloud LLC GDPR interpretation. You are encouraged to complete your own GDPR interpretation

UnifyCloud

Controller's (or your customer's) GDPR compliance model

**European Council
Council of the European Union**

GDPR Regulation (261 pages)

43 GDPR Requirements*

1. Provide notice of processing activities at the time personal data is obtained.

2. Provide notice of processing activities if personal data has not been obtained directly.

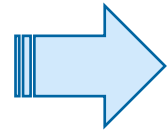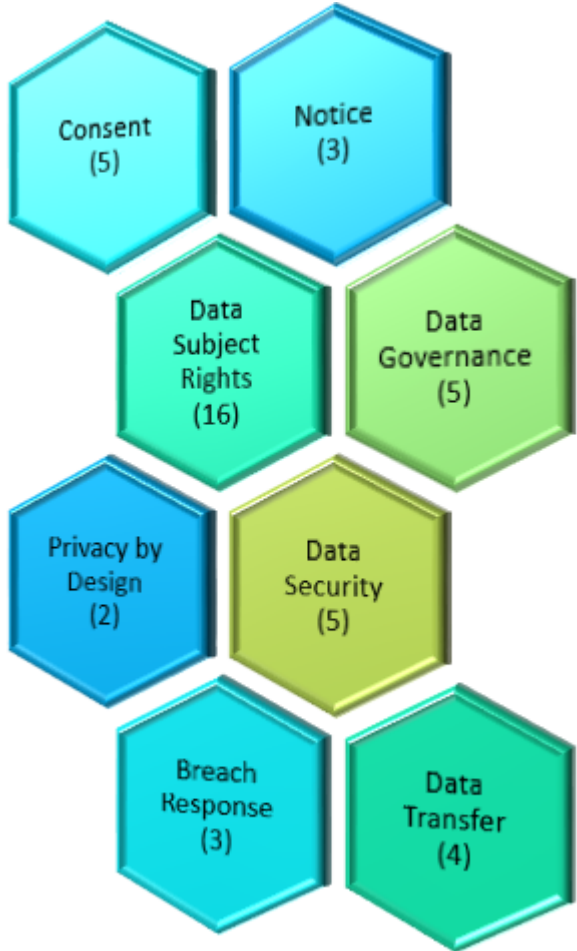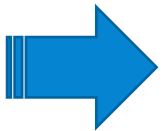3. Provide the data privacy notice at all points where personal data is collected.

* UnifyCloud LLC GDPR interpretation. You are encouraged to complete your own GDPR interpretation

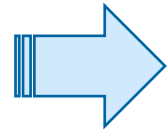UnifyCloud

Controller's (or your customer's) GDPR compliance model

**European Council
Council of the European Union**

GDPR Regulation (261 pages)

43 GDPR Requirements*

- Consent (5)
- Notice (3)
- Data Subject Rights (16)
- Data Governance (5)
- Privacy by Design (2)
- Data Security (5)
- Breach Response (3)
- Data Transfer (4)
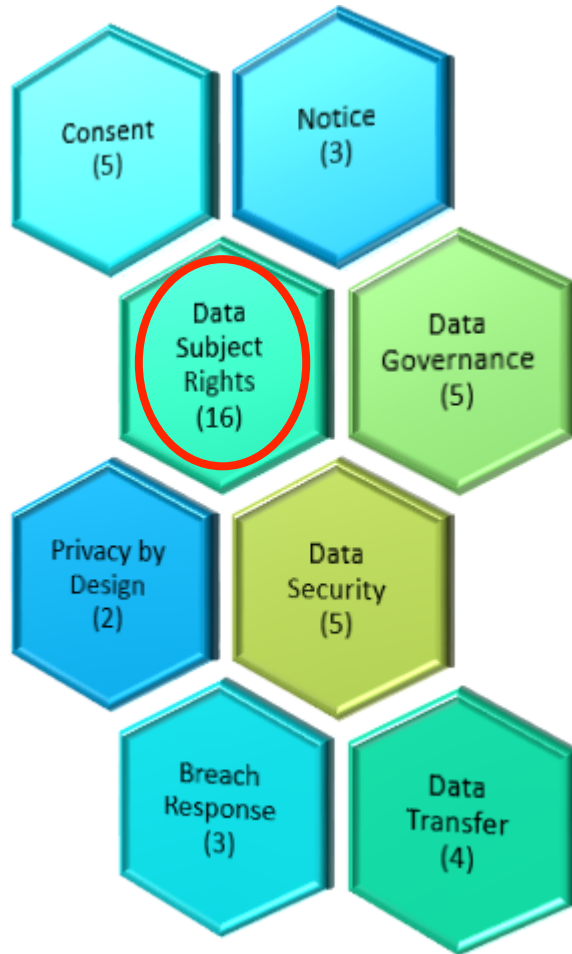
1. Provide mechanism for validating identity of the requesting data subject.

2. Provide mechanism for to request access to their personal data.

3. Provide a mechanism to respond to requests on personal data access.

4. Maintain the technological ability to trace and search personal data.

5. Provide mechanism to request rectification and rectify personal data.

6. Provide a mechanism to request the erasure of personal data.

7. Maintain the technological ability to locate and erase personal data.

8. Track to which additional controllers personal data has been transferred.

* UnifyCloud LLC GDPR interpretation. You are encouraged to complete your own GDPR interpretation

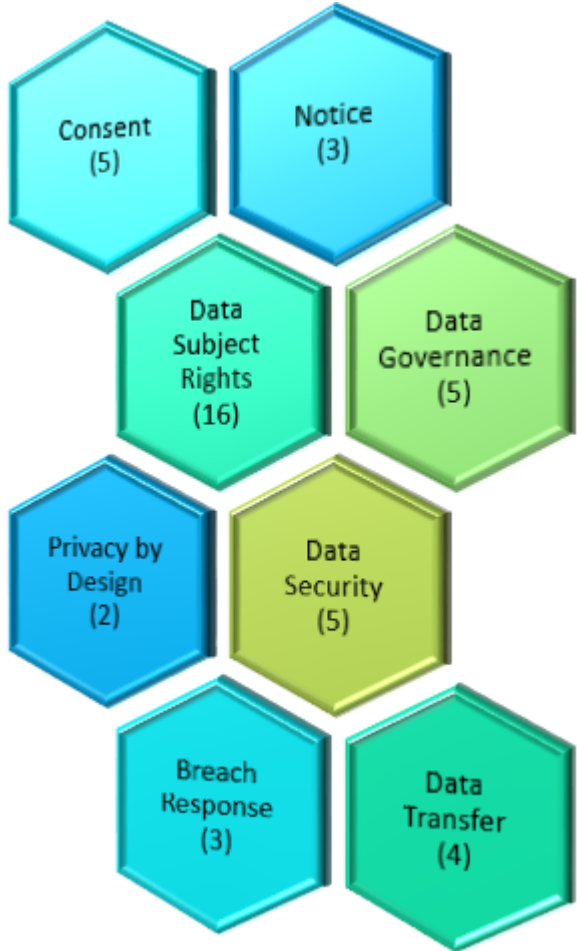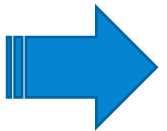UnifyCloud

Controller's (or your customer's) GDPR compliance model

43 GDPR Requirements*

GDPR Regulation (261 pages)

Consent (5)

Notice (3)

Data Subject Rights (16)

Data Governance (5)

Privacy by Design (2)

Data Security (5)

Breach Response (3)

Data Transfer (4)
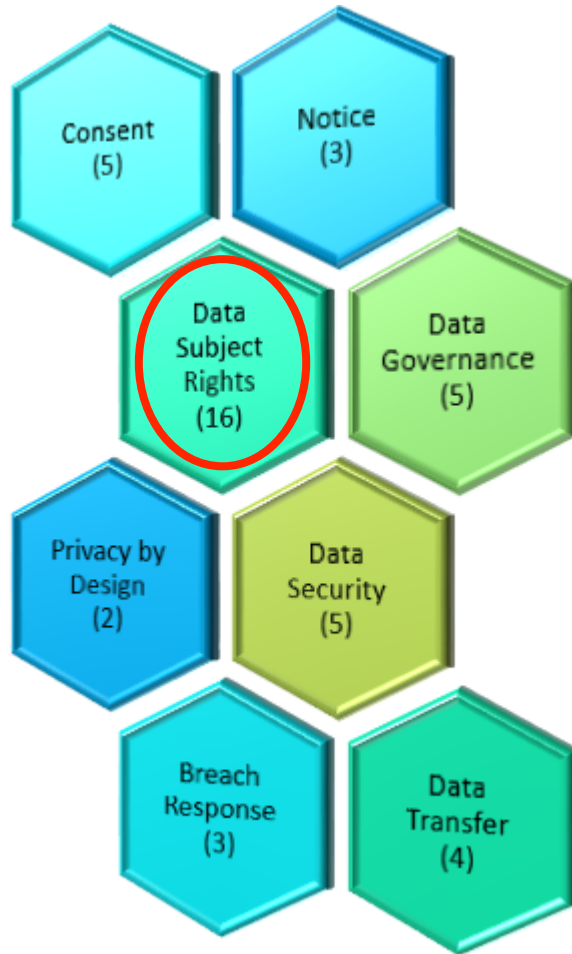
9. When personal data is made public, contact those entities for data erasure.

10. Provide mechanism to request the restriction of data processing.

11. Maintain the technological ability to restrict processing of personal data.

12. Provide mechanism to request copies and transmit personal.

13. Provide mechanism to respond to data portability requests.

14. Locate personal data and export in structured, machine-readable formats.

15. If processing for direct marketing, provide mechanism to object.

16. Maintain the technological ability to discontinue the data processing.

* UnifyCloud LLC GDPR interpretation. You are encouraged to complete your own GDPR interpretation

UnifyCloud

Controller's (or your customer's) GDPR compliance model

European Council
Council of the European Union

43 GDPR Requirements*

GDPR Regulation (261 pages)
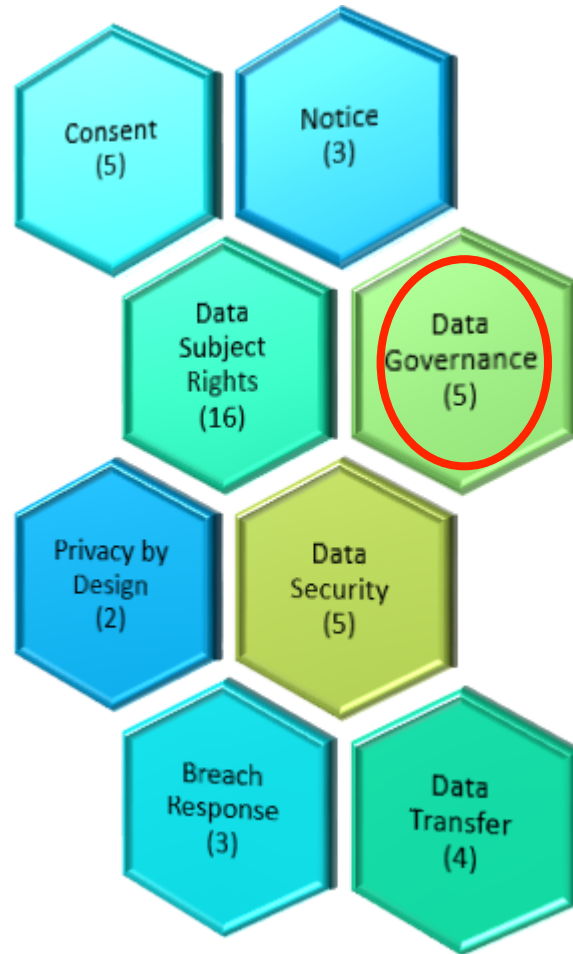
1. Maintain audit trails to demonstrate accountability and compliance.

2. Maintain inventory of data detailing categories of data subjects.

3. Maintain auditable trails of processing activities.

4. Carry out data protection impact assessments of processing operations.

5. Provide the de-identification of personal data for archiving purposes.

* UnifyCloud LLC GDPR interpretation. You are encouraged to complete your own GDPR interpretation

UnifyCloud

Controller's (or your customer's) GDPR compliance model

European Council
Council of the European Union

GDPR Regulation (261 pages)

43 GDPR Requirements*

1. Embed privacy controls (in service and development lifecycle).

2. Embed privacy designed to minimize the amount of personal data collected.

* UnifyCloud LLC GDPR interpretation. You are encouraged to complete your own GDPR interpretation

UnifyCloud

Controller's (or your customer's) GDPR compliance model

European Council
Council of the European Union

43 GDPR Requirements*

GDPR Regulation (261 pages)

Consent (5)

Notice (3)

Data Subject Rights (16)

Data Governance (5)

Privacy by Design (2)

Data Security (5)

Breach Response (3)

Data Transfer (4)

1. Provide mechanism to pseudonymize, encrypt, or otherwise secure personal data.

2. Implement security measures in the service.

3. Confirm ongoing confidentiality, integrity, and availability of personal data.

4. Provide mechanism to restore the availability and access to personal data.

5. Facilitate regular testing of security measures.

* UnifyCloud LLC GDPR interpretation. You are encouraged to complete your own GDPR interpretation

UnifyCloud

Controller's (or your customer's) GDPR compliance model

European Council
Council of the European Union

GDPR Regulation (261 pages)

43 GDPR Requirements*

1. Controllers notify DPA within 72 hours in the event of a data breach incident.

2. Controllers notify affected data subjects of a high-risk data breach incident.

3. Processors notify controllers without undue delay of a data breach incident.

* UnifyCloud LLC GDPR interpretation. You are encouraged to complete your own GDPR interpretation

Controller's (or your customer's) GDPR compliance model

European Council
Council of the European Union

GDPR Regulation (261 pages)

43 GDPR Requirements*

- Consent (5)
- Notice (3)
- Data Subject Rights (16)
- Data Governance (5)
- Privacy by Design (2)
- Data Security (5)
- Breach Response (3)
- Data Transfer (4)
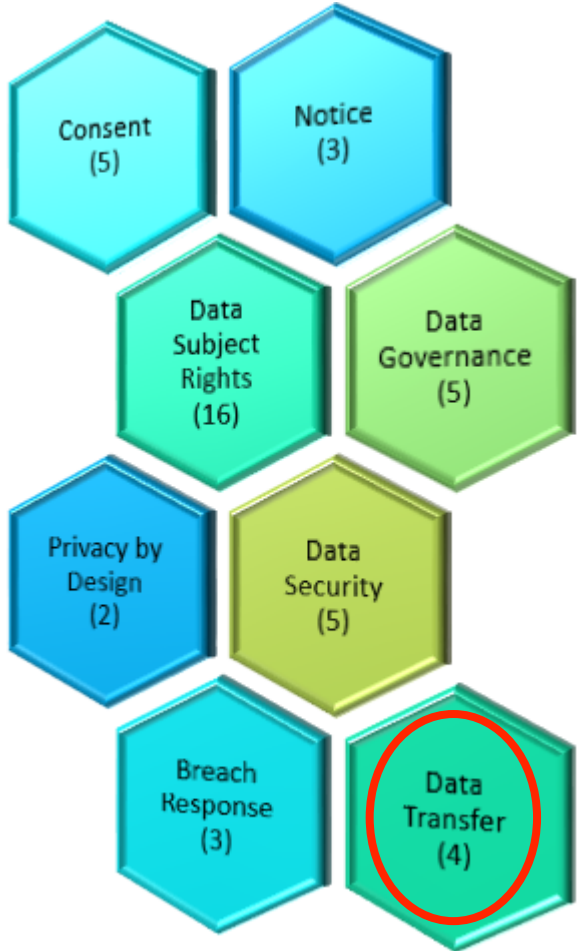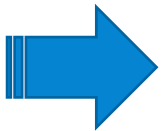
1. Track and record personal data that is forwarded to third-parties.

2. Provide mechanism for tracking and recording data transfers in and out of the EU.

3. Maintain inventory of data transfer contracts with third-parties.

4. Provide appropriate safeguards (e.g., Privacy Shield) for effective legal remedies.

* UnifyCloud LLC GDPR interpretation. You are encouraged to complete your own GDPR interpretation

UnifyCloud

Controller's (or your customer's) GDPR compliance model

Controller's (or your customer's) GDPR compliance model

European Council
Council of the European Union

GDPR Regulation (261 pages)

Consent (5)

Notice (3)

Data Subject Rights (16)

Data Governance (5)

Privacy by Design (2)

Data Security (5)

Breach Response (3)

Data Transfer (4)

Cloud Compliance Model ?

Business Processes & User Controls

SaaS Applications & Workload Features

Cl...re

CLOUD SERVICES

Internal Audit

SOC 2 Type 2

SOC 1 Type 2

ISO 27018

ISO 27001

UnifyCloud

Controller's (or your customer's) GDPR compliance model

European Council
Council of the European Union

Cloud Compliance Model ?

GDPR Regulation (261 pages)

Consent (5)

Notice (3)

Data Subject Rights (16)

Data Governance (5)

Privacy by Design (2)

Data Security (5)

Breach Response (3)

Data Transfer (4)

Business Processes & User Controls

Microsoft Enterprise Mobility Suite
Symantec
Blue Coat
skyhigh
netskope

SaaS Application
workday
box
salesforce
Dynamics 365
Office 365
Dropbox
SAP Cloud Platform
Ultimate SOFTWARE

amazon web services
Microsoft Azure
Rackspace HOSTING
Google Cloud Platform
IBM CLOUD SERVICES
Alibaba Cloud
ORACLE CLOUD
CenturyLink Technology Solutions
virtustream

Internal Audit

"So a dashboard through which your team can easily track that (capabilities) will come in handy."

Source: *Brief: You Need An Action Plan For The GDPR*; Forrester Research; October 2016

AICPA SOC
AICPA SOC

SOC 2 Type 2
SOC 1 Type 2

ISO
ISO 27001

ISO 27018
ISO 27001

UnifyCloud

Poll:
How many cloud services providers do you have?

UnifyCloud

Understanding a Cloud shared responsibility model for GDPR

Source: *Amazon Web Services*

Source: *Microsoft*

What "managed by customer" means (from a typical SOC* report)…

Controls and reporting as well as configuration oversight **_excluded_** from a CSV platform SOC report

- Controls over account / subscription IDs and passwords and access to applications.

- Compliance with applicable laws/regulations.

- Determining and implementing encryption for data.

- Securing certificates used to access applications.

- Selection of access mechanism for data.

- Determining the Services configurations.

- Backup of data to local / Cloud storage.

- Protection of the secrets associated with accounts.

- Implementing interconnectivity between Cloud and on-premises resources.

- Security Development Lifecycle for applications.

- Application QA prior to moving to Cloud production.

- Monitoring the security of applications.

- Reviewing and applying public security and patch updates (IaaS).

- Reporting the incidents and alerts specific to systems and subscriptions.

- Support timely responses with Cloud platform.

- Implementing redundant systems for hot-failover.

* AICPA Service Organization Control (SOC) Reports (Type I and Type II)
   formerly Statement on Auditing Standards No. 70: Service Organizations (SAS 70)

UnifyCloud

Using a GDPR baseline approach

Controls and reporting as well as configuration oversight **_excluded_** from a CSV platform SOC report

- Controls over account / subscription IDs and passwords and access to applications.
- Compliance with applicable laws/regulations.
- Determining and implementing encryption for data.
- Securing certificates used to access applications.
- Selection of access mechanism for data.
- Determining the Services configurations.
- Backup of data to local / Cloud storage.
- Protection of the secrets associated with accounts.

- Implementing interconnectivity between Cloud and on-premises resources.
- Security Development Lifecycle for applications.
- Application QA prior to moving to Cloud production.
- Monitoring the security of applications.
- Reviewing and applying public security and patch updates (IaaS).
- Reporting the incidents and alerts specific to systems and subscriptions.
- Support timely responses with Cloud platform.
- Implementing redundant systems for hot-failover.

An Cloud Service GDPR Baseline should include:

- Cloud Services Compliance Validation (ISO, SOC)
- Services Setting Values
- DevOps Rules for Cloud Services

Impact on Security

What impact will DevOps have on the security of production systems?

- 15% Systems will be much more secure
- 36% Systems will be somewhat more secure
- 26% It will have no impact on security
- 4% Systems will be somewhat less secure
- 1% Systems will be much less secure
- 18% Don't know
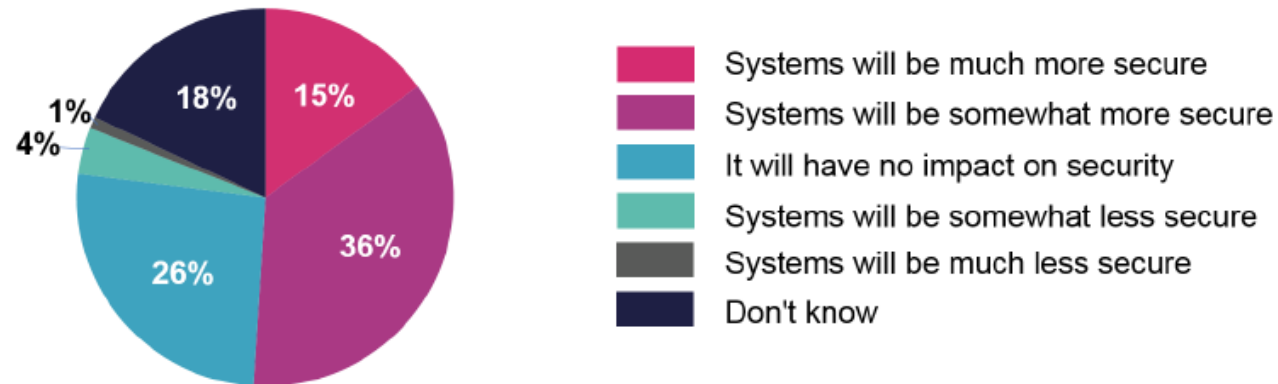
Base: 237 respondents who have adopted or plan to adopt DevOps
Data: UBM survey of 300 IT professionals involved in applications, January 2017

Figure 9

"However, in terms of security, while few respondents reported a decrease in production security, this is an area where DevOps has not yet contributed significant improvement. (See Figure 9) This may not be the fault of DevOps practices themselves–increasing security requires a deliberate effort–but it could point to an opportunity for tools vendors."

UnifyCloud

Case Study: GDPR Baseline Dashboard for Azure

- 130 deployable Azure Services (last count)
- Some Services are candidates for GDPR defined "personal & sensitive data""
  o Blob Storage
  o Data Factory
  o Data lake Store
  o SQL Database
  o SQL Data Warehouse
  o StorSimple
- Some Services are capabilities to help meet GDPR requirements:
  o Azure AD
  o Azure Information Protection
  o Key Vault
  o Multi-factor Authentication

Azure Services and GDPR compliance roles

S.No.	Cloud Service	High Level Description (from Capstone GDPR White paper)	Journey Stage				Compliance	
			Discover	Manage	Protect	Report	Enabler	Target
1	Active Directory	An identity and access management solution in the cloud. It manages identities and controls access to Azure, on-premises, and other cloud resources, data, and applications. With Azure Active Directory Privileged Identity Management, you can assign temporary, Just-In-Time (JIT) administrative rights to eligible users to manage Azure resources.		Yes	Yes		Yes	
2	Key Vaults	It offers an easy, cost-effective way to safeguard keys and other secrets in the cloud by using hardware security modules (HSMs). Protect cryptographic keys and small secrets like passwords with keys stored in HSMs.			Yes		Yes	
3	Storage Account (Classic)	An Azure storage account gives you access to the Azure Blob, Queue, Table, and File services in Azure Storage. Your storage account provides the unique namespace for your Azure Storage data objects. By default, the data in your account is available only to you, the account owner.		Yes				Yes
4	Data Factories	It is a managed service which lets you produce trusted information from raw data in cloud or on-premises sources. Easily create, orchestrate and schedule highly-available, fault-tolerant work flows of data movement and transformation activities.		Yes				Yes
5	Multifactor Authentication	It helps prevent unauthorized access to on-premises and cloud applications by providing an additional layer of authentication. Follow organizational security and compliance standards while also addressing user demand for convenient access.			Yes		Yes	
6	Site Recovery	It helps you protect important applications by coordinating the replication and recovery of private clouds for simple, cost-effective disaster recovery.			Yes		Yes	
7	SQL Service	It is a relational database-as-a service using the Microsoft SQL Server Engine. SQL Database is a high-performance, reliable, and secure database you can use to build data-driven applications and websites in the programming language of your choice, without needing to manage infrastructure.		Yes	Yes			Yes

UnifyCloud

GDPR baseline setting guidance for Azure Services

S.No.	Cloud Service	CloudOrigin Functionality	Value	Subject	GDPR Citation	Issue
1	Active Directory	Active Directory -> Integration with local AD -> Domains verified for Directory Sync	1	Data Subject Rights	Art. 15-17	Provide mechanism for validating identity of the requesting data subject.
		Active Directory -> Integration with local AD -> Domains planned for Single Sign-On	0	Data Subject Rights	Art. 15-17	Provide mechanism for validating identity of the requesting data subject.
		Active Directory -> Integrated Applications -> Users may give applications permission to access their data	NO	Right to Restriction	Art. 18, Sec. 1, Sub. (a) – (d)	Maintain the technological ability to restrict processing of data subjects' personal data (or for Microsoft customers to do so in accordance with requests of data subjects).
		Active Directory -> Integration with local AD -> Directory Sync	Activated	Data Security	Art. 32, Sec. 1, Sub. (a)	Provide mechanism to pseudonymize, encrypt, or otherwise secure personal data.
		ACTIVEDIRECTORY_INTEGRATEDAPPLICATIONS_USERSMAYADDINTEGRATEDAPPLICATIONS	No	Data Subject Rights	Art. 15-17	Provide mechanism for validating identity of the requesting data subject.
		ACTIVEDIRECTORY_USERACCESS_ALLOWINVITATIONS	Yes	Right to access	Art. 15, Secs. 1 – 2	Provide mechanism for data subjects to request access to their personal data and receive information on the processing activities of their personal data.
		ACTIVEDIRECTORY_USERACCESS_ALLOWGUESTSTOINVITE	No	Right to access	Art. 15, Secs. 1 – 2	Provide mechanism for data subjects to request access to their personal data and receive information on the processing activities of their personal data.
		ACTIVEDIRECTORY_USERACCESS_LIMITGUESTACCESS	Yes	Right to access	Art. 15, Secs. 1 – 2	Provide mechanism for data subjects to request access to their personal data and receive information on the processing activities of their personal data.

UnifyCloud

Creating a GDPR baseline

Creating a GDPR baseline

Creating a GDPR baseline

Creating a GDPR baseline

Monitoring a GDPR baseline

Monitoring a GDPR baseline

Monitoring a GDPR baseline

Monitoring a GDPR baseline

Summary

- GDPR is in effect now and will be enforced starting on May 25, 2018

- Cloud solutions (IaaS/PaaS and SaaS) will be part of a controller's compliance model

- Understand / interpret the GDPR requirements and map to processor features / controls

- Consider using a GDPR baseline approach for areas where certifications do not apply

- For vendors...do **NOT** imply using your solution will directly guarantee GDPR compliance

- Thank you! Any final questions?

UnifyCloud

The GDPR and Its Implications On Cloud Services

September 2017

Norm Barber, Managing Director
(normb@unifycloud.com)

A copy of this presentation will be made available to you after the session ends. Visit www.cloudatlasinc.com for additional information about our solutions.

UnifyCloud

script

Data Governance, Ethics and the law

Ethics and law: why does it matter to computer scientists?

Costs: fines and reputation

BOYCOTT

SONY BMG

"In encoding the discs [with copy-protection spyware] Sony and F4i have decided that their intellectual property is more deserving of protection than the intellectual property and personal information on millions of personal computers around the world"

— Excerpt of class-action lawsuit filed against SONY BMG and First 4 Internet, US District court, New York, 11/14/2005

script

No Buy-in by needed users

Loss of trust

- Fines (under GDPR: a fine up to 10,000,000 EUR or up to 2% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater (Article 83, Paragraph 4 [14]))
- a fine up to 20,000,000 EUR, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher (Article 83, Paragraph 5 &

- Damages: potentially unlimited

- Data breach notification duty:here goes your reputation
-

Ethics and Data science

- A bit like kissing in the school yard:
- Lots of people seem to be talking about it
- Much fewer actually do it
- Even fewer do it well

script

What does „data ethics" mean?

- Don't break the law?
- Don't break the spirit of the law?
- Don't do harm (non-malevolence)?
- Do good (benevolence)
- Respect autonomy?
- Be just?
- Be a „good X" (scientists, doctor, politician etc)
  - Noe be bad

What does professional ethics mean

- Being a „good X" (scientists, administartor, judge…)
- Not violating the professional rules
- Being perceived by others as exemplary
- Being a „virtuous" X

The knowledge trifeca

- Known risks („known kowns")
- Known possible risks („known unkown")
- Unknown but real risks (unkonwn unkowns")

Known risks and the law

- Privacy
- Property (IP)
  - Commercialisation and independence
  - Benefit sharing
- Openness
  - FOI
  - Funding council guidelines: open access, replicability

Risk Management and planning tools I

- SWOT
  - *strengths*, *weaknesses*, *opportunities*, *threats*
- PEST
  - political, economic, social and technological
- PESTLE
  - political, economic, social, tech; legal; ethical
- STEEPLE (D)
  - Environemntal and demographic
- SPELIT,
  - legal and intercultural factors

Risk management and planning tools II

- Privacy Impact Assessment
- Cabinett Office Big Data Analysis Tool

Cabinett Office Data Ethics Tool

1 Start with clear user need and public benefit

2 Use data and tools which have the minimum intrusion necessary

3 Create robust data science models

4 Be alert to public perceptions

5 Be as open as possible

6 Keep data secure
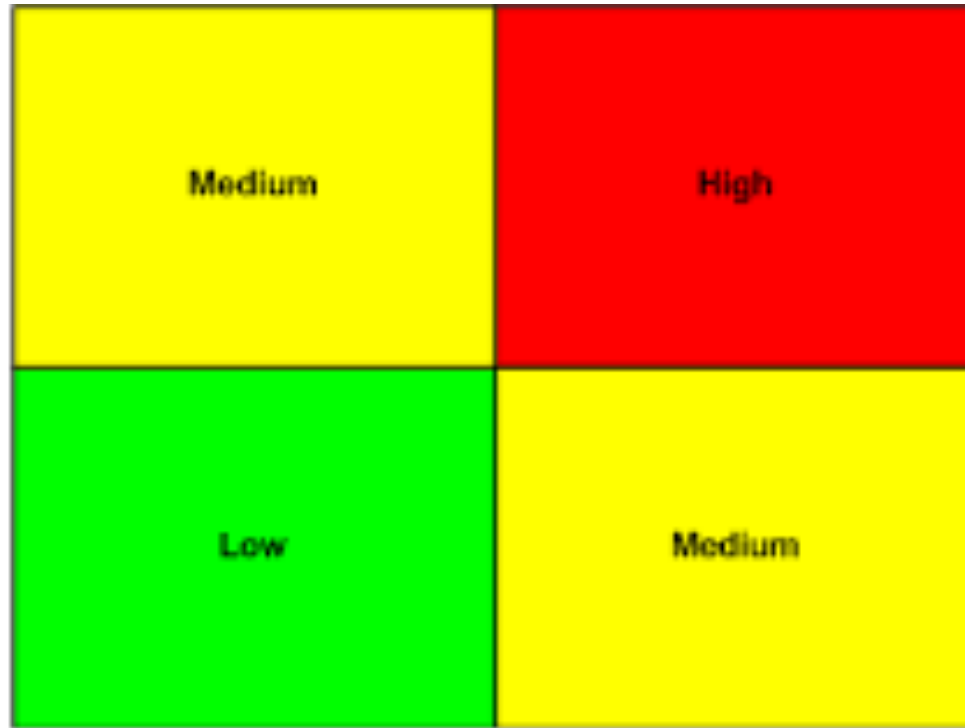
Case studies

The bad

- US university applicants apply for federal grants

- One section of the application form asks them to rank their universities by preferenes

Step Six (Student): Indicate which colleges you want to receive your FAFSA information.

Enter the six-digit federal school code and your housing plans. You can find the school codes at **www.fafsa.gov** or by calling 1-800-4-FED-AID. If you cannot get the code, write in the complete name, address, city and state of the college. For state aid, you may wish to list your preferred college first. To find out how to have more colleges receive your FAFSA information, read **What is the FAFSA?** on page 10.

	1ST FEDERAL SCHOOL CODE		NAME OF COLLEGE / ADDRESS AND CITY	STATE	HOUSING PLANS
101.a		OR			101.b on campus ◯ 1 / with parent ◯ 2 / off campus ◯ 3
101.c	2ND FEDERAL SCHOOL CODE	OR	NAME OF COLLEGE / ADDRESS AND CITY	STATE	101.d on campus ◯ 1 / with parent ◯ 2 / off campus ◯ 3
101.e	3RD FEDERAL SCHOOL CODE		NAME OF	STATE	101.f on campus ◯ 1

- Form is then shared with universities
- ...which in some cases use this to reject candidates that did not list them first
- Maybe worse, offered less financial suport to candidates who listed them second
- Combined with browsing data from ranking websites

- Data minimisation?
- Data sharing?
- Consent, secondary use/purpose binding principle
- Harming your clients?
- Non-sustainable/harming your future data access

- Privacy
- Harm to the person who supplies the data

The racist sentencing support system

The Legal System Uses an Algorithm to Predict If People Might Be Future Criminals. It's Biased Against Blacks.

And it's terrible at predicting future crimes.

BY JULIA ANGWIN, JEFF LARSON, SURYA MATTU AND LAUREN KIRCHNER, PROPUBLICA   MAY 23, 2016 5:16 PM

TOP NEWS

A Black Woman Is Arguing a Big Supreme Court Case Today.

script

- Discrimination
- Violation of laws
- Hidden biases
- Wider social harm

The ugly

Facebook's mood study: How you became the guinea pig

That controversial research into how posts affect users' emotions is just latest in a long line of privacy flaps -- and apologies -- for the social networking giant.

Internet

July 1, 2014
7:45 AM PDT

by *Seth Rosenblatt*
🐦 @sethr

When news spread over the weekend that Facebook had manipulated its news feed to study how social media posts affect people's emotions, the real surprise was that anyone was that surprised.

The study (PDF), published in the Proceedings of the National Academy of Sciences and
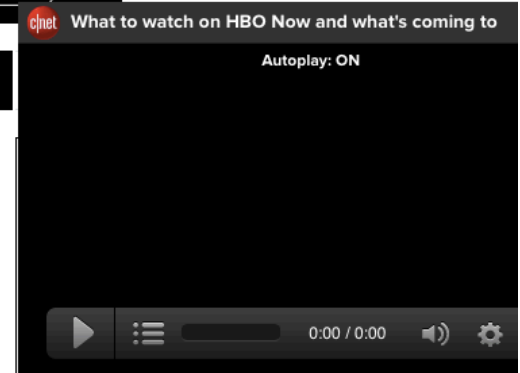
- Privacy
- Autonomy
- Benefits? Justice?

The good?

Citizen science – where could be the harm in that?

- Citizens record noise levels on mobile phones
- City makes planning decisions on that basis
  - (traffic calming/redirection measures)

- Who is heard and who is not heard?
- Who suffers from the decision taken?

The good?

Cloudteams

OUR MISSION IS TWO-FOLD

1

OPEN UP THE DEVELOPMENT PROCESS

If you are a software design & developer team, CloudTeams will offer useful tools to collaborate with potential customers, get their feedback and stream it effectively into the work cycle. We believe this will help you become more competitive and offer great applications to the world.

2

ENJOY BETTER APPLICATIONS

If you think software applications should be meaningful and enjoyable, CloudTeams will offer you a way to actively collaborate with creators to shape up any type of software application. We believe that with the right set of tools, transparency & control people like you can make a difference.

- Earn points while you share
- Get earlier/cheaper/free access to the apps that are developed
- Make the most of your Facebook account by combining it with CT data

Possible issues

- Is gameification appropriate for health data?

- Risk through cumulative participation with same development team

- Risk of inducing you to violate your obligations

Organisations

Bott Chapter 3

Becoming a Legal Entity

- Types of organisation: commercial, public, not-for-profit.
- Mostly we look at commercial organisations intended to make profits.
- Different kinds of organisation:
  - Sole trader – individual – no legal formalities – the legal entity is the individual.
    - If turnover is big enough will need to register for VAT etc.
    - The individual is liable for company debts – so assets like home, savings are at risk
  - Partnership – this is the form a group must trade under unless it is a limited company
    - Often the required form of organisation for professionals e.g. law, medical, hedge fund etc because the liability issues control excesses
    - Liability is joint and several liability – all are fully liable for the debt of the partnership
  - Limited company : the preferred form of legal entity for commercial firms

Limited companies

- Three principles:
  - The company is a legal person separate from the people who own or work in the company.
  - Ownership is divided into shares that can be bought and sold by shareholders
  - Owners of the company have no obligation to pay debts incurred by the company – the owners risk is limited to the value of their shares.
- In the UK:
  - Public limited company (plc): public can hold shares – BA plc – shares may or may not be listed on the stock exchange
  - Private limited company (Ltd): shares cannot be held by the public -Small Company Ltd

Setting Up a Limited Company

- Two documents:
  - Memorandum of Association: short and simple – name, location of the registered office, objects of the company, liability clause (saying the limits to liability of the owners), share capital (e.g. 100 shares, value £1 – to be a plc must have capital over £50K). Concludes with declaration of association that list the people setting up the company.
  - Articles of Association: Complex and technical (see the handout). Covers how the company will run, roles of directors, …
- Once a company is registered then the memo of association and articles of association are on public deposit at Companies House.

Directors

- Sometimes shareholders run the company but in larger companies directors may be employed
- Directors must:
  - Have regard to the owners and employees' interests
  - Act in good faith and for the benefit of the company
  - Exercise skill and care (be "professional")
  - Declare conflicts of Interest
  - Legally:
    - Be aware of the financial position of the company
    - Drawing up annual reports and accounts and filing them at companies house
    - Complies with relevant law

- Companies have executive (employed) and non-executive (non-employed advisors)
- Every company has a company secretary responsible for required communications

Conflicts of Interest – Activity – Reading

- Individually, read clause 14 of the model articles
- In pairs look again at clause 14(4) parts (a)-(c)
- Choose one each of (a) – (c) and try to explain it to your partner
- Write down your explanations.
- Get together in a group of four
- Review your explanations – choose the best one and then work together to write a short scenario describing when you think that clause might be invoked in an imaginary company.

Setting up a company

- Not necessary to employ a lawyer or accountant
- Easiest way is to buy an "off-the-shelf" company and tailor it to your needs (change the name, objectives, constitution, …)
- Registering a company yourself costs £100 (same-day service at the Register of Companies) – this is slower because you need to fill in forms etc.
- UK and US have similar, easy, ways to set up companies. In other countries it can take several months and cost thousands of pounds.

Non-Commercial Bodies

- Statutory bodies – set up by act of Parliament e.g. local unitary authorities.
- Royal Charter: sets up free-standing bodies that are independent of the state, e.g. Universities
- Not-for-profit organisations (often established as companies limited by guarantee):
    - Charities
    - Professional organisations: BCS, Institute of Physics, …
    - Political Parties

Summary

- Becoming a legal entity
- What situations are different entities appropriate
- Limited companies
- Obligations on limited companies
- Other organisations

Organizations, Structure, Management

Bott Chapter 4

ORGANIZATIONAL MODELS

Organizational Models

- Organizational Theory (founded by Max Weber on the theory side) developed the **bureaucratic model**:
  - Tasks are split into specialist roles and people become expert in these
  - Each rule is precisely specified so one expers can be substituted for another
  - Each individual is accountable to one manager who directs their work
  - Employees are required to relate to each other and customers in a formal and impersonal way.
  - Recruitment is based on qualification, employees are protected from arbitrary sacking, promotion is based on seniority and achievement
- **Organic Model** (Likert): "… ensure a maximum probability that in all interactions and in relationships within the organisation, each member, in the light of their background, values, desires and expectations, will view the experience as supportive and one which builds a sense of personal worth and importance" – small professional companies.

Matrix Model

- Accepts that bureaucratic model is too restrictive

- Work may be project-based

- Employees may be working on several projects simultaneously

- Employees may answer to several managers at once

Organogram
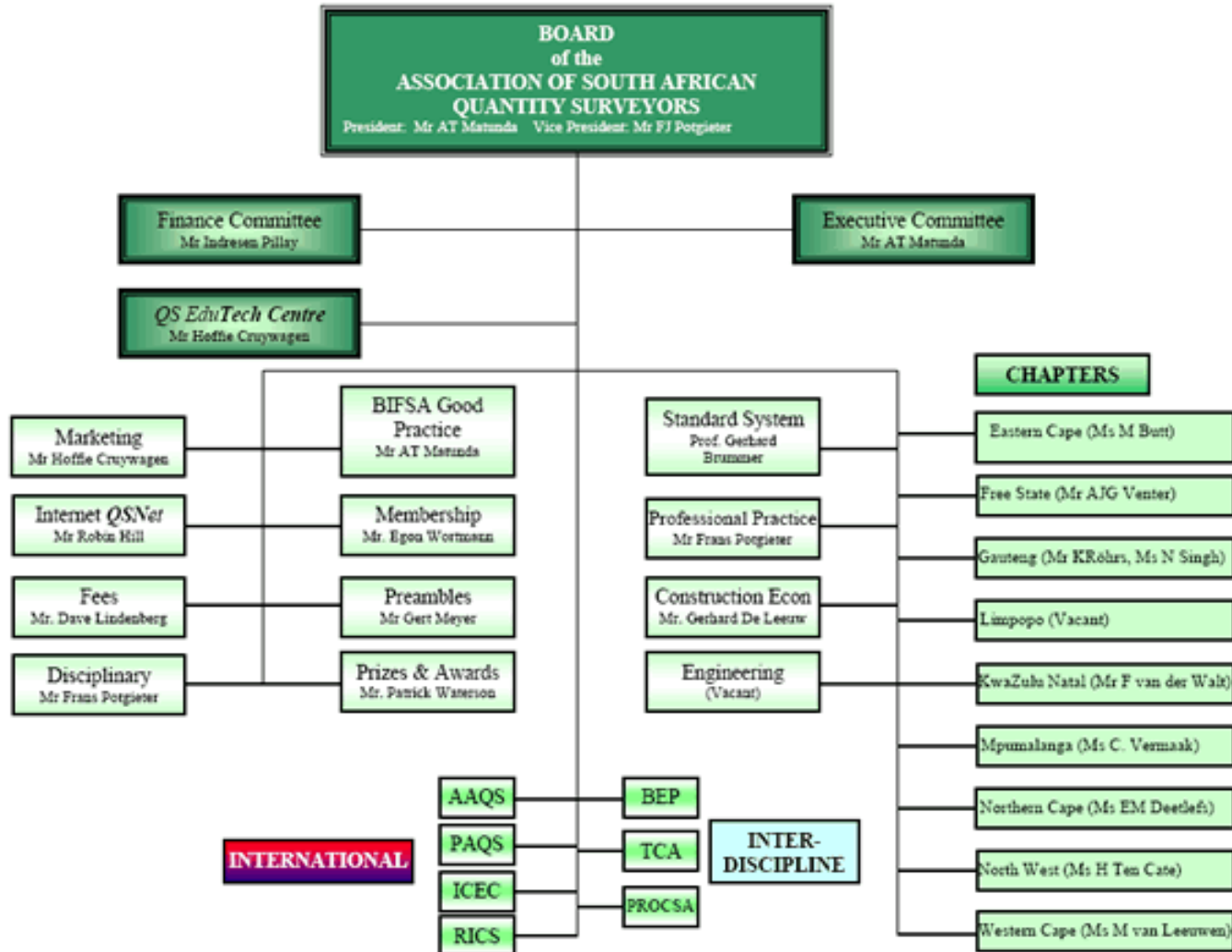
Organogram
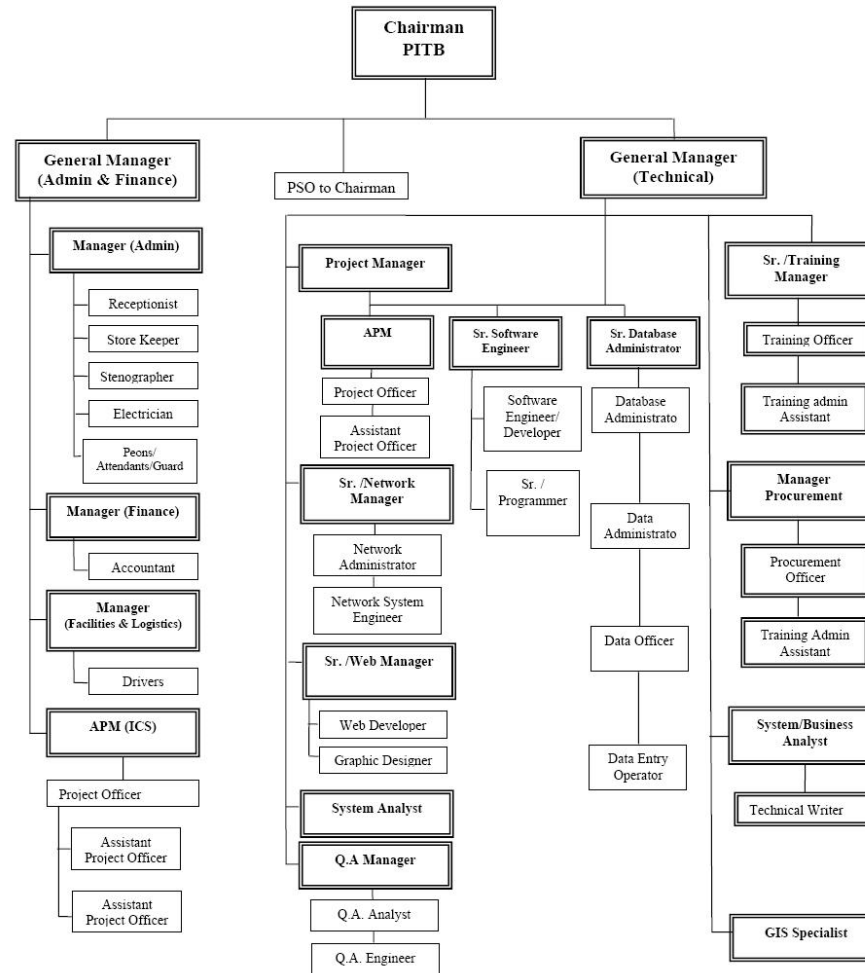
Organogram

ORGANOGRAM G2 ANGLO AMERICAN CORPORATION—SUMMARISED ORGANOGRAM, 1992. (After elimination of control structures, including Amic.) *Source:* Kaplan & Stewart
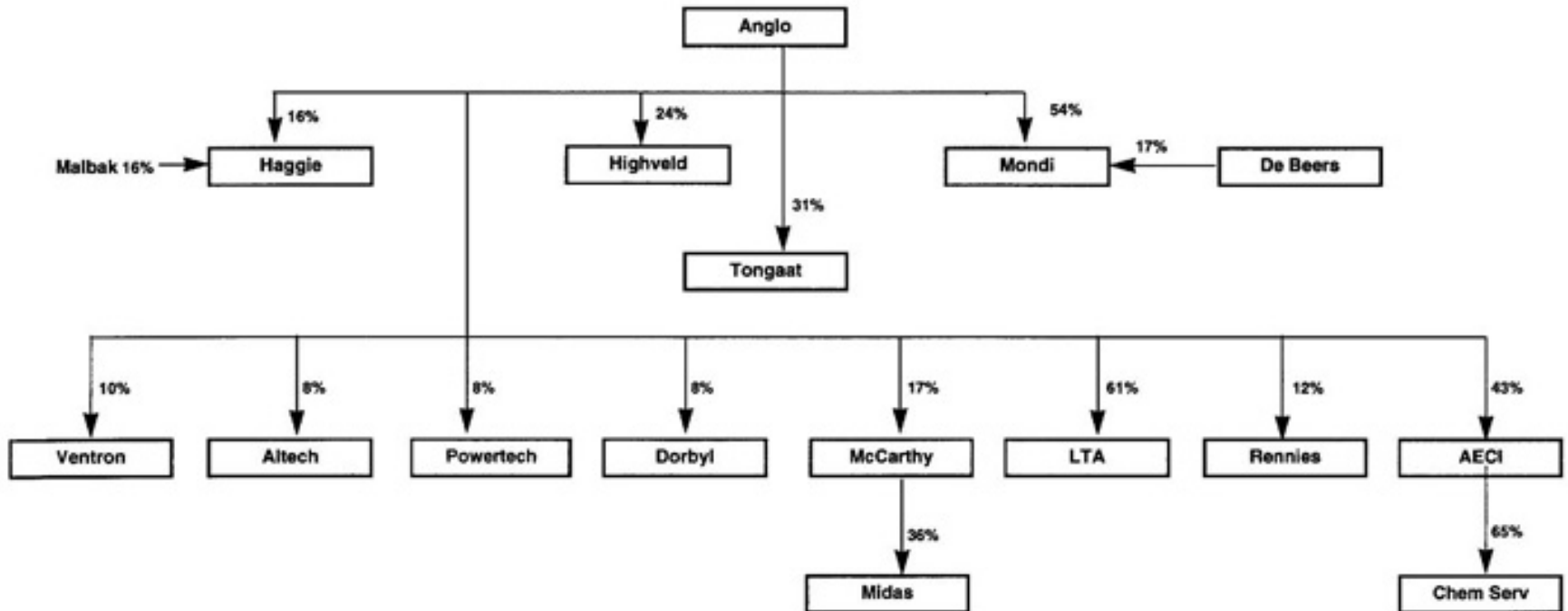
Organogram
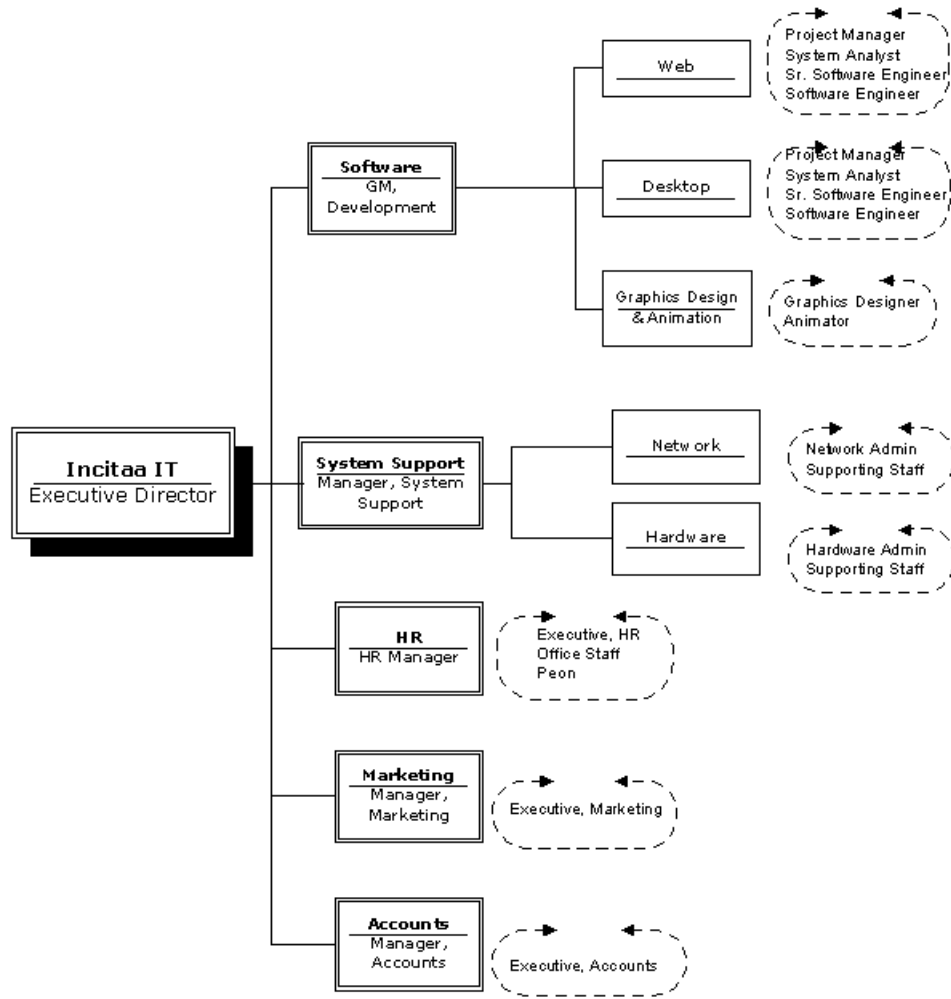
Organogram

City District Government Rawalpindi Organogram

- Chairman RDA
- District Nazim
- District Assembly
- District Police Office
- District Coordination Officer
  - EDO Finance & Planning
  - EDO Revenue
  - EDO Education
  - EDO Health
  - EDO Information Technology
  - EDO Works & Services
  - EDO Law
  - EDO Literacy
  - EDO Municipal Services
  - EDO Agriculture
  - EDO Community Development
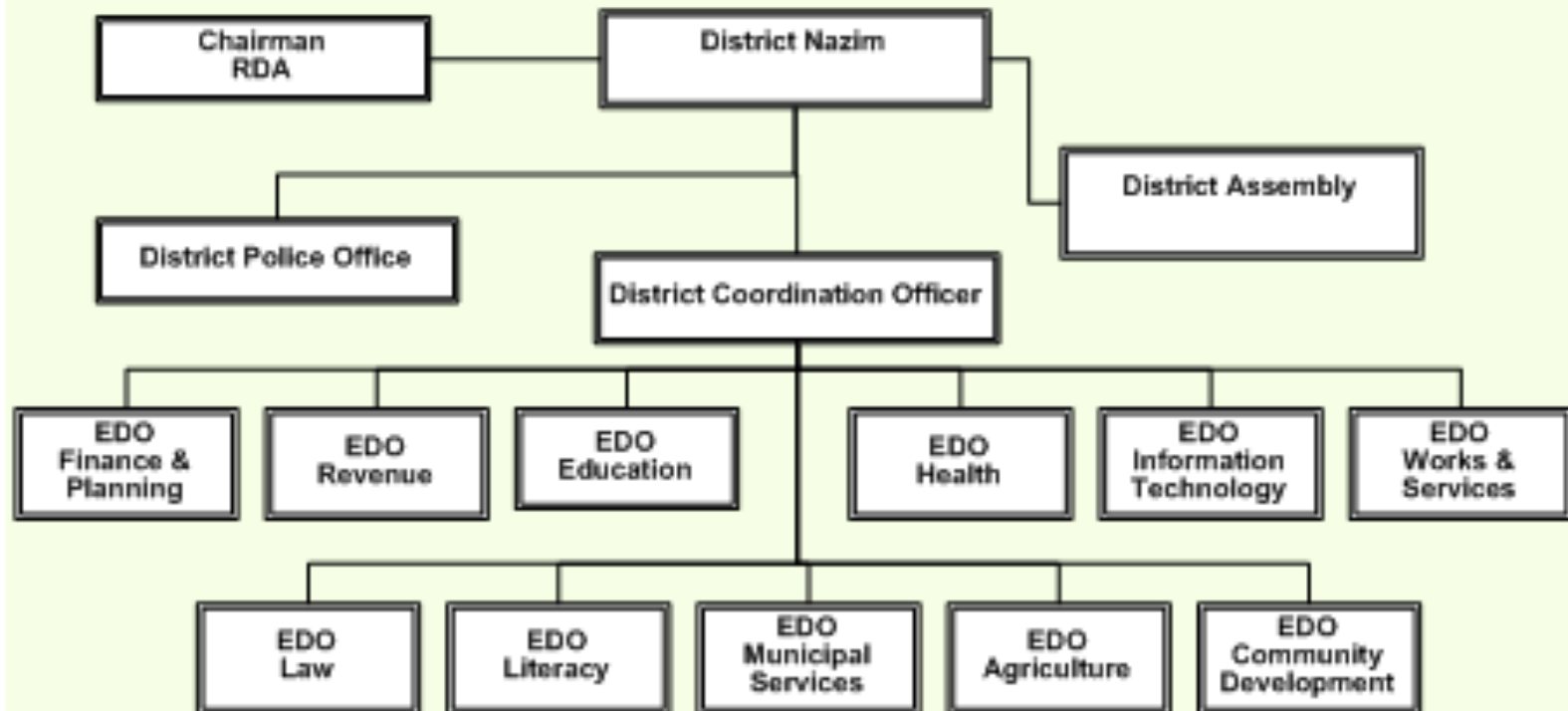
Organogram
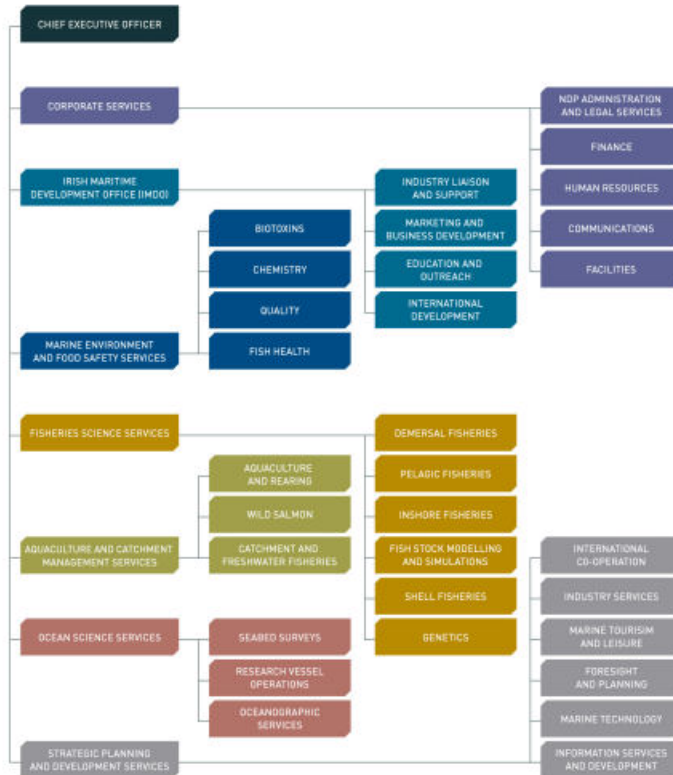
Activity

- On your own: draw up a list of potential organisational structuring principles.
- In a pair, refine your list with your partner and:
  - Identify two structuring principles that could be used together
  - Identify two structuring principles that do not combine well
- In a group of 4 refine the list further and come up with your best pair of principles that work together and the pair that do not work together. Try to think of a company that could use the pair you suggest in each case.

Some Structuring Principles

- Function
- Geography
- Ownership
- Product Line
- Technology
- Operational Structure
- Depth of Hierarchy
- Centralised versus decentralised
- What structure is appropriate to the size of company?

Guardian on VW Dieselgate

Graham Ruddick

Thursday 17 December 2015 12.34 GMT

Volkswagen has made sweeping changes to its senior management team as it attempts to cut costs and overhaul its culture following the diesel emissions scandal.

The German carmaker has almost halved the number of senior managers reporting directly to Matthias Müller, the chief executive, and brought in several new faces.

Müller has pledged to transform the notoriously unwieldy structure of VW after the company admitted that the emissions scandal had occurred because of a "whole chain" of errors and a corporate mindset that tolerated rule-breaking.

He said the management changes would "speed up the decision-making process, reduce complexity and increase efficiency".

VW Response to Dieselgate

- Key elements of the process optimization are:
  - Early documentation and interpretation of legislation around the world and alignment of the product portfolio with the legal requirements
  - Guidelines for the development of software for drive control units with documentation of the features with relevance for registration
  - Introduction of multiple controls for approvals in the product development process
  - **Reorganization within Development for the purpose of separating the responsibility for the development of drives from official approvals**
  - **Formation of new bodies for cross-brand management and clarification of compliance issues**
  - Uniform process standards and work instructions that give those involved legal certainty in the work process
  - Training programs in which everyone involved in the process is required to participate
  - Regular reporting to the Group Board of Management in order to create transparency in relation to the implementation status of this process optimization

Summary

- Organisational structure is essential for larger organisations

- Structure according to business priorities

- All business structures make it difficult for the organisation to respond to some risks.

- Structure to facilitate business and make it easy to respond to the most likely serious risks

MANAGERS AND LEADERS

Managers and Leaders

- One day you might want to be a manager or a director
  - What does that *mean* exactly?
  - What issues should you be sensitive to?
    - Depends on your seniority

Pause for Thought

- Managers and Leaders
- In pairs, what would you expect of:
  - A manager
  - A leader
- In terms of:
  - The activity they carry out.
  - Their personal characteristics and skills.

The Manager

- Develops plans and timetables
- Organises
- Delegates and monitors
- Exercises control, applies corrective action
- Communicates
- Motivates
- Delivers (predictable)
- Looks inwards

Leader can emerge …

- Perceived by group as most competent in leadership functions -

- Task-orientated: coordinating, initiating contributions, evaluating, information seeking and giving, opinion seeking and giving, motivating

- Socio-emotional: reconciling differences, arbitrating, encouraging participation, increasing cohesion

The Leader

- Establishes direction
- Develops vision
- Communicates and inspires vision
- Energises others
- Innovates
- Figurehead, Spokesman
- Looks outwards

Summary

- Managers manage, leaders lead
- Managers have a specific role within the organisational structure:
  - Replaceable
  - Trainable
- Leaders provide direction, may arise from anywhere:
  - Not easily replaceable
  - Not trainable

CONTROLLING ORGANIZATIONS

Organisation

- A company is an instrument for maximising value for the shareholders

- Driven by markets – lack of understanding of market = no customers = no business

- Driven by resources – lack of understanding = lack of control

- The more senior you become the more these will be concerns

Performance areas (Drucker)

- Market standing
- Innovation
- Productivity
- Physical and financial resources
- Profitability
- Worker performance and attitudes
- Manager performance and development
- Public responsibility

Markets and Marketing

- Marketing is <u>not</u> stuff through your letter-box or people cold-calling you at 6pm.

- Marketing is the business of understanding the market, your place in it, your opportunities, threats, competition and your customers

- There exist many tools and models to help understand them

Porter's 5 forces

New Entrants

Barriers to entry →

Suppliers → Competitors ← Buyers

↑
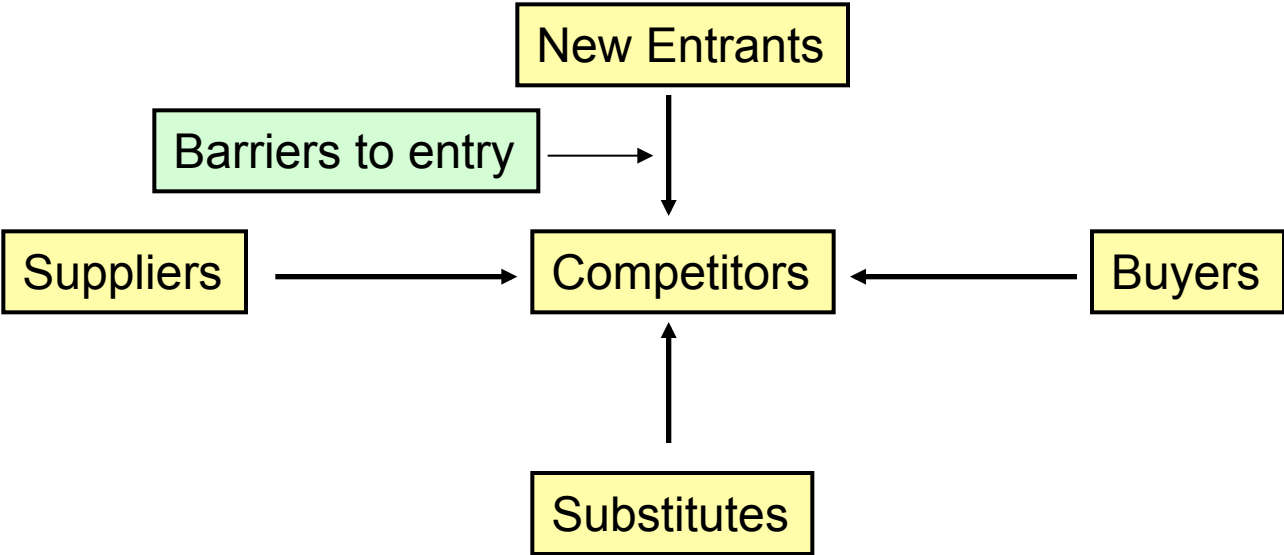
Substitutes

Examples

- New Entrant: Ford - Tesla
- Substitute: Vinyl record – CD – iTunes - Spotify
- Control of suppliers – Tesco
- Control of buyers – monopoly
- Control by buyers – perfect market; eBay?

- Barriers to entry – Semiconductor industry – mobile phones…

P.E.S.T. / S.W.O.T.

- Political
- Economic
- Social
- Technological

- Strengths
- Weaknesses (internal)
- Opportunities
- Threats (external)

P.E.S.T. – car market

- Political – emissions reduction targets
  - Works against internal combustion engines
- Economic – control of rare earth production
  - Raises concerns over electric vehicles
- Social – family size, behaviour
  - 1-parent families – hatchbacks?
  - Millenials: Transport as a service
- Technological – new products
  - Hydrogen, hybrids, recyclable materials

Marketing Mix – the 4 * Ps

- Product
  - Quality, features, name, packaging, services, guarantee
- Price
  - List price, discounts, credit
- Promotion
  - Advertising, personal selling
- Place
  - Distributors, retailers, locations, transport

Competition

- Can compete on *cost o*r *differentiation:*
  - Cost: make the same thing cheaper
  - Differentiation: make it different / better / here
- Competitiveness based on core competencies
  - Anyone can make Coca-Cola
    - Only they have the network of licensed manufacturers and distributors (and the brand name)
  - Anyone can put an aircraft in the sky
    - Only the profitable airlines can fill it every time
- Each survivor is uniquely superior to all others in some way and thus occupies a niche

Breakout

You are a horse-buggy whip manufacturer ca. 1910

Consider the market you are in, perform a PEST and SWOT analysis and indicate what market repositioning might be advantageous

S.W.O.T.

Horse-buggy whip manufacturer, 1910 sees horses making way for cars

- Strength: has supply chain to reach buggy owners / future car owners
- Weakness: product is horse-dependent
- Threat: cars make product obsolete
- Opportunity: reposition as supplier of driver accessories

Actually they didn't and went out of business

Market repositioning

- McDonalds
- Royal Bank of Scotland
- Burberry
- Apple

Data...

How Fortune 1000 Executives Report Using Big Data
The projects they've started, and where they're finding value.

	Started and seen value	Started and not seen value	Not started
Decrease expenses	49.2%	23.4%	27.4%
Find new innovation avenues	44.3	20.2	35.5
Launch new products/services	36.1	26.8	37.1
Add revenue	32.8	22.0	45.2
Increase the speed of current efforts	31.1	33.4	35.5
Transform business for the future	27.9	23.7	48.4
Establish a data-driven culture	27.9	41.5	30.6
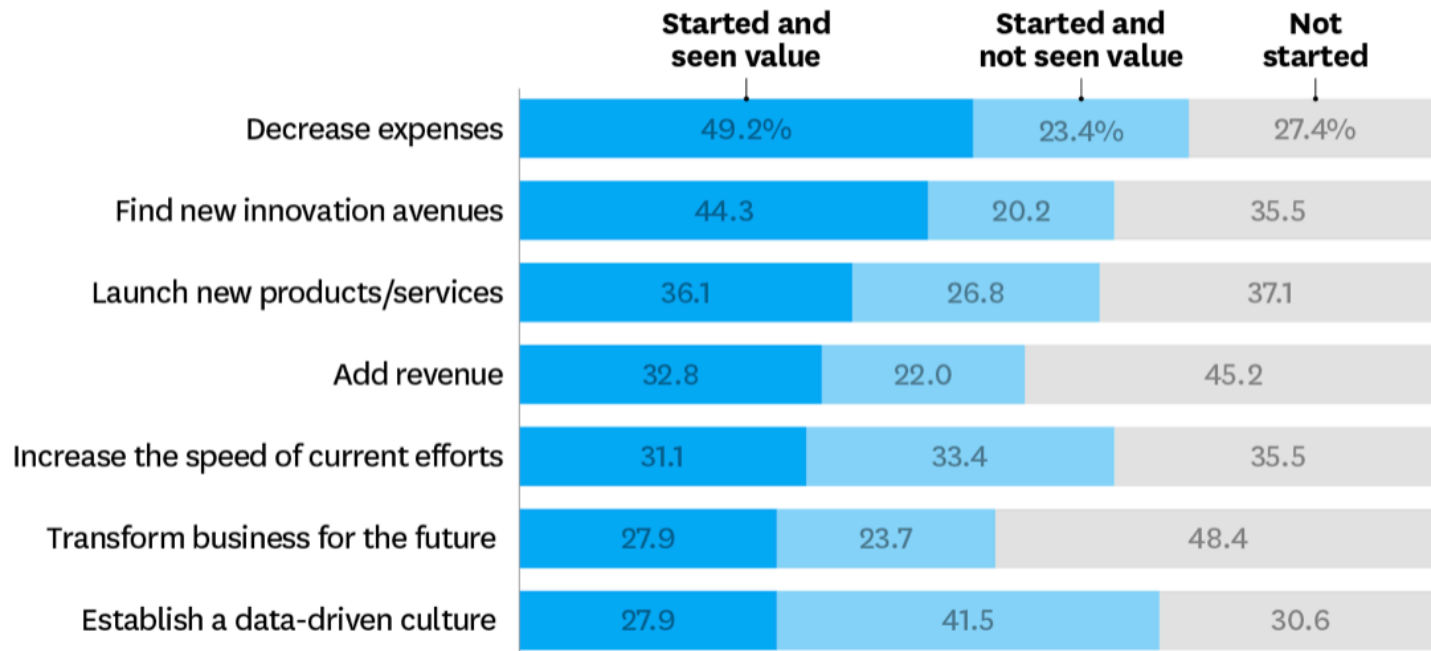
Summary

- Successful organizations know their markets
- Successful organizations are sensitive to changes in markets
- Successful organisations measure what is going on in markets
- Companies use data to support strategic decisions (and this is changing rapidly).

Equality and Technology?

Dr. Karen Gregory
Lecturer in Digital Sociology
k.gregory@ed.ac.uk

The Promise of Tech

- What type of digital world are we building? Why?

- How do technological developments mirror social values or social structures?

- Who does technology "work" for? Why?

- What is the relationship between education and the world we design and develop?

Coding crisis?

You Retweeted

Brian Mastenbrook @bmastenbrook · Oct 31

Not a crisis: not everybody can code.

Actually a crisis: programmers don't know ethics, history, sociology, psychology, or the law.

↩   ⇄ 5.8K   ♥ 11K   •••

Mastenbrook is CTO of AirStash, IoT Platform

Diversity in Tech

Employee breakdown of key technology companies

		GENDER		ETHNICITY					
		Female	Male	White	Asian	Latino	Black	Multi	Other
USA	population	51		64	4	16	12	1	3
social	facebook	31		57	34	4	2	3	
	flickr	37		50	39	4	2	2	2
	Google+	30		61	30	3	2	4	1
	Instagram	31		57	34	4	2	3	
	LinkedIn	39		53	38	4	2	2	1
	Pinterest	40		50	42	2	1		5
	tumblr	37		50	39	4	2	2	2
	twitter	30		59	29	3	2	3	4
	YouTube	30		61	30	3	2	4	1
tech	amazon	37		60	13	9	15		3
	apple	30		55	15	11	7	2	1
	DELL	30		69	9	11	10		1 (US)
	eBay	42		61	24	5	7	1	1
	Google	30		61	30	3	2	4	1
	hp	33		72	6	14	7	1	1
	intel	25		61	26	9	4		1 (US)
	NVIDIA	16		38	44	3	1	14	1
	YAHOO!	37		50	39	4	2	2	2
vs.	Top 50 US companies	46		68	10	10	12	no data	no data (US)
most diverse US company	Kaiser Permanente		76	48	20	18	13	no data	no data
	US Congress	19		80	6	6	8	no data	no data (US)
	Venture Capitalists	11		87	9	2	2	2	no data (US)
	Fortune 500 CEO's	5		83	2	2	1	no data	no data (US)

	GENDER		ETHNICITY					
	Female	Male	White	Asian	Latino	Black	Multi	Other

InformationIsBeautiful.net

part of project: Knowledge is Beautiful

- Although the proportion of managers at U.S. commercial banks who were Hispanic rose from 4.7% in 2003 to 5.7% in 2014, **white women's representation dropped from 39% to 35%, and black men's from 2.5% to 2.3%**.

- Among all U.S. companies with 100 or more employees, the **proportion of black men in management increased just slightly—from 3% to 3.3%—from 1985 to 2014**.

- White women saw bigger gains from 1985 to 2000—rising from 22% to 29% of managers—**but their numbers haven't budged since then**.

- Even in Silicon Valley, where many leaders tout the need to increase diversity for both business and social justice reasons, bread-and-butter tech jobs remain dominated by white men.

Source: Quotes taken from Harvard Business Review. 2016. "Why Diversity Programs Fail."

So What?

- Why does this matter?

  - Job demand. Estimated 1.4 million tech jobs by 2020. (29% US; of that 29% only 3% will be women)
  - The research shows that mixed-gender teams are more innovative, more creative and more productive.
  - Companies with a diverse group of employees make more money.
  - Companies with women in leadership positions have higher profits, higher sales and higher rates of revenue growth.

- "You are not your user." Can one social demographic design for a complex world?

- More broadly, what is the relationship between discrimination in tech and discriminatory systems?

(Source: "Women Technologists Count: Recommendations and Best Practices to Retain Women in Computing. Anita Borg Institute, 2013)

Beyond Diversity?

- Response to this phenomena has been "diversity" training and "diversity initiatives", but recent research suggests:
    - The positive effects of diversity training rarely last beyond a day or two, and a number of studies suggest that it can activate bias or spark a backlash.
    - Managers and employees react negatively to "mandatory trainings." Voluntary training has marginally better success rates.
    - Diversity testing has resulted in "cherry picking" results, which amplifies bias.
    - Performance ratings and ranking have also been found to amplify bias.
    - Data driven, "control" solutions may compound existing inequalities and interpersonal bias.

(Source: Harvard Business Review. 2016. "Why Diversity Programs Fail.")

Gains for whom?

LEAN IN
WOMEN, WORK, AND THE WILL TO LEAD
SHERYL SANDBERG
THE INTERNATIONAL BESTSELLER

- Solutions must go deeper and speak to culture, social relations, and labor practices.

- Making room for more than "different" bodies, but complexity of experience and understanding of the world.

Some Definitions

- Prejudice: A positive or negative cultural attitude.

- Bias: Implicit or Explicit? Gender bias & racial bias.

- Stereotypes: associations, and attributions of specific characteristics to a group

- Ra*cism*, Se*xism*, Clas*sism*: Ideology, or a system of ideas.

- Discrimination: bias behavior or action taken toward

- Intersectional understanding: Double Jeopardy

Source: Dovidio, et al. 2010. "Prejudice, Stereotyping and Discrimination: Theoretical and Empirical Overview" in *The Sage Handbook of Prejudice, Stereotyping and Discrimination*. London: Sage.

Implicit Bias

- "Unconscious" bias. Unintentional or "human condition"?

- Design interventions, such as in Orchestra experiment. There is a tendency in implicit bias work to want to outsource judgment.

- Can data be less biased than the human who produce or analyze the data?

Psychology & Sociology

- But, is there a better way to understanding inequality and how it is socially reproduced?

- To that end, I thought we would look at the technology industry as a pipeline. And take a look at the sociological picture at each stage.

The "Digital Divide" & Education

- "The demographic factors most correlated with home broadband adoption continue to be educational attainment, age, and household income."
- 74% of white adults have broadband Internet at home while 64% of African American and 53% of Latino adults do.
- 89% of those with a college degree have broadband at home; 57% of high school graduates and 37% of those without a high school diploma do.
- 88% of those who earn more than $75,000 have broadband at home; just 54% of those who earn less than $30,000 a year do.

(Source: Pew Research, "Home Broadband", 2013)

Reasons people do not have broadband at home

In April of 2009, 7% of American adults age 18+ used dial-up internet at home. (As of August 2011, this number is 3%.) These are the reasons they gave for not switching to broadband.

	% of dial-up users
What would it take to get you to switch to broadband?	
Price must fall	35%
Nothing would get me to switch	20
Don't know	16
It would have to become available where I live	17
Other	13

Higher Education & Gender
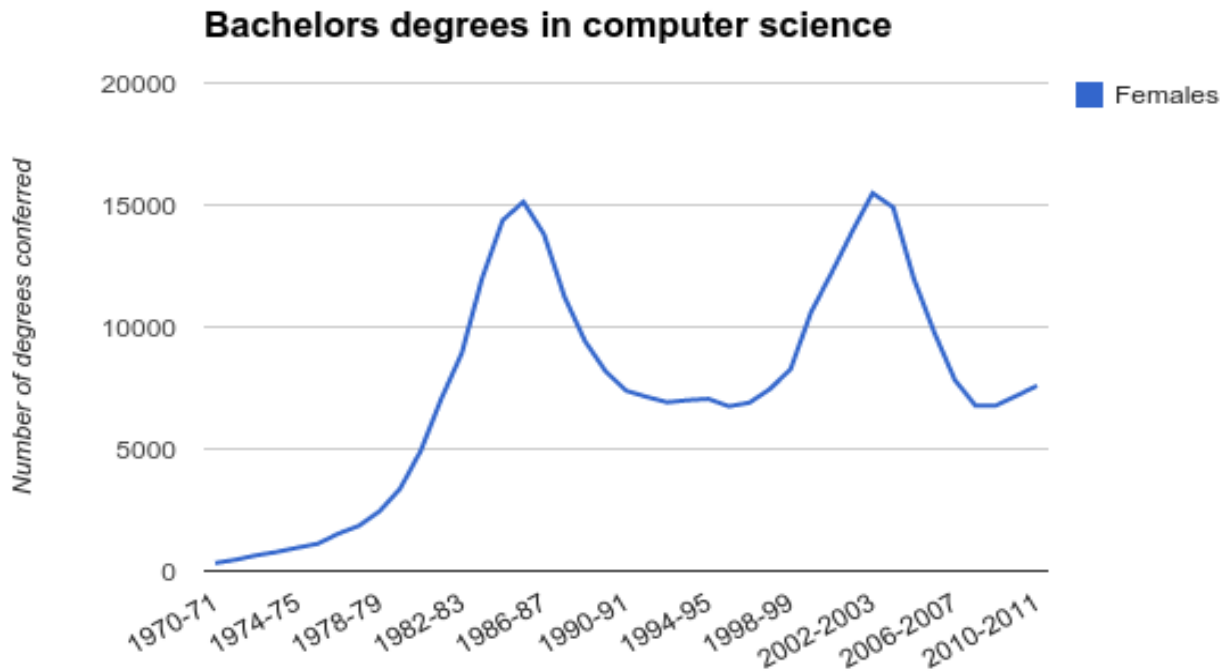
Bachelors degrees in computer science

"The central conclusion is that the first personal computers were essentially early gaming systems that firmly catered to males. While early word processing tools were also available, the marketing narrative told the story of a new device that met the needs of men.

As more males began purchasing computers for personal use, the "nerdy programmer" classification began to take hold in the professional world of computer science. By the mid-nineties, the percentage of women studying computer science at the postsecondary level had fallen to 28%."

- Poor preparation and lack of encouragement in STEM subjects in school also contributes to a lack of women in STEM fields.

- The classroom climate for girls in school classrooms and for women students and faculty in university departments has been classically described as "chilly" (Hall & Sandler 1982).

- A dearth of role models: Women students look to faculty as role models for balancing career and family, and if career demands are seen as excessive, may leave their department in higher numbers than men (Ferreira 2003).

- Lack of "critical mass" of women in a department may lead to dissatisfaction and greater attrition of women scientists (Dresselhaus et al. 1995; Ferreira 2003).

- Salary gap and work-life balance issues already deter women in college.

Hiring Practices

"Over the past few years, we have been working hard to increase diversity at Facebook through a variety of internal and external programs and partnerships. We still have a long way to go, but as we continue to strive for greater change, we are encouraged by positive hiring trends.

For example, while our current representation in senior leadership is **3% Black, 3% Hispanic and 27% women**, of new senior leadership hires at Facebook in the US over the last 12 months, 9% are Black, 5% are Hispanic and 29% are women."– Maxine Williams, Director of Global Diversity, Facebook

Workplace Practices

- If women find themselves in workplaces where colleagues or bosses assume they're less competent than men.

- Typically they work longer hours than their male colleagues, and cut back outside-work activities, which may lead to burnout.

- Women are likelier than men to suffer from imposter syndrome.

- Tech culture is hostile or even harassing.

- It may be harder for women to attend industry events than it is for men, because of personal obligations.

- There aren't very many female mentors, sponsors or role models.

- Women are impeded from forming strong professional networks to the extent those networks ordinarily form around gendered pursuits such as sports, or activities that may be risky for a lone woman among men such as getting drunk.

These quotes are taken from "Why Women Leave Tech" compiled by Sue Gardner:
https://docs.google.com/document/d/1soIYek-YEIvqtu9brv3ecdPbuVzQKp_GhAozC06UrLo/edit#

Career Trajectory

- Career "Plateau" and lack of advancement.

- Women leave tech in mid-30s, when men's careers begin to develop.

- Not only "work-life balance" or family… as they leave for other jobs outside of tech industry.

(source: The Athena Factor: Reversing the Brain Drain in Science, Engineering, and Technology, 2008)

The percentage of women working in the major tech companies is remarkably consistent at around 30 percent. But a closer look at the breakdown of females in leadership or technical roles shows significantly fewer women in positions to influence their companies' product development or strategic direction.

Overall 29.1%

Includes Google, Apple, Facebook, Microsoft, Intel, Cisco, Twitter and Amazon

Company	Percentage
Amazon	37%
Facebook	31%
Google	30%
Apple	30%
Twitter	30%
Microsoft	29.1%
Intel	24%

Tech 15.6%

Includes Google, Apple, Facebook, Microsoft, Cisco and Twitter

Company	Percentage
Apple	20%
Google	17%
Microsoft	16.6%
Facebook	15%
Twitter	10%

Leadership 22.5%

Includes Google, Apple, Facebook, Microsoft, Twitter and Amazon

Company	Percentage
Apple	28%
Amazon	25%
Facebook	23%
Google	21%
Twitter	21%
Microsoft	17.2%
Intel	16%
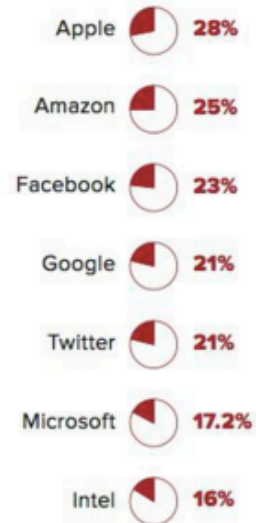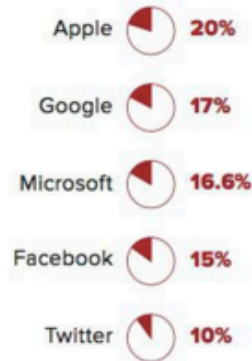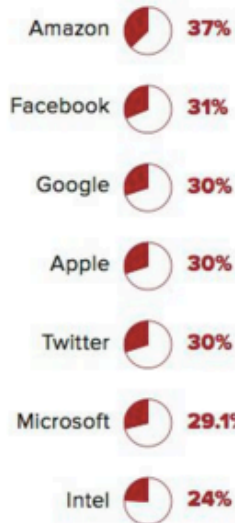
Social Effects: From Apps to Social Systems

- SketchFactor: An app to allow users to report having seen or experienced something "sketchy" in a particular location; these reports would then be geotagged and overlaid on a Google map, creating a sketchiness heat map of a neighborhood or city.

Marantz, A. 2015. "When An App is Called Racist." The New Yorker: http://www.newyorker.com/business/currency/what-to-do-when-your-app-is-racist

- Noble, S. 2013. "Google Search: Hyper-visibility as a Means of Rendering Black Women and Girls Invisible." *InVisible Culture: An Electronic Journal for Visual Culture*. http://ivc.lib.rochester.edu/google-search-hyper-visibility-as-a-means-of-rendering-black-women-and-girls-invisible/

- Try searching for "professor" in Google:

https://www.google.co.uk/search?q=professor&safe=strict&espv=2&biw=1440&bih=721&source=lnms&tbm=isch&sa=X&ved=0ahUKEwjsiMDUx4zQAhWJCcAKHU3BAGUQ_AUIBigB

- Bivens, R. and Haimson, O. 2016. "Baking Gender Into Social Media Design: How Platforms Shape Categories for Users and Advertisers." *Social Media + Society*. October-December: 1–12. http://sms.sagepub.com.ezproxy.is.ed.ac.uk/content/2/4/2056305116672486.full.pdf+html

- Zukin, S., Lindeman, S. and Hurson, L. 2015. "The Omnivore's Neighborhood: Online restaurant reviews, race, and gentrification." *Journal of Consumer Culture*.

- The study suggests that Yelp reviews not only reflect the impacts and public perception of gentrification, but ultimately help to determine who occupies a neighborhood as well. Indeed, the study concludes that, "intentionally or not, Yelp restaurant reviewers may encourage, confirm, or even accelerate processes of gentrification by signaling that a locality is good for people who share their tastes." Beyond persuading potential customers to visit a restaurant, social media may in fact be part of the process of actually transforming neighborhoods.

- Angwin, J. and Parris, T. 2016. "Facebook Lets Advertisers Exclude Users by Race: Facebook's system allows advertisers to exclude black, Hispanic, and other "ethnic affinities" from seeing ads." *ProPublica: Journalism in the Public Interest.* https://www.propublica.org/article/facebook-lets-advertisers-exclude-users-by-race

"In an experiment on Airbnb, we find that applications from guests with distinctively African-American names are 16% less likely to be accepted relative to identical guests with distinctively White names. Discrimination occurs among landlords of all sizes, including small landlords sharing the property and larger landlords with multiple properties. It is most pronounced among hosts who have never had an African-American guest, suggesting only a subset of hosts discriminate. While rental markets have achieved significant reductions in discrimination in recent decades, our results suggest that Airbnb's current design choices facilitate discrimination and raise the possibility of erasing some of these civil rights gains."

- Edelman, B., Luca, M. and Svirsky, D. 2016. "Racial Discrimination in the Sharing Economy: Evidence from a Field Experiment"

Court ruling on November 1, 2017:

http://www.nytimes.com/2016/11/02/technology/federal-judge-blocks-racial-discrimination-suit-against-airbnb.html

- "Passengers have faced a history of discrimination in transportation systems. Peer transportation companies such as Uber and Lyft present the opportunity to rectify long-standing discrimination or worsen it. We sent passengers in Seattle, WA and Boston, MA to hail nearly 1,500 rides on controlled routes and recorded key performance metrics. Results indicated a pattern of discrimination, which we observed in Seattle through longer waiting times for African American passengers—as much as a 35 percent increase. In Boston, we observed discrimination by Uber drivers via more frequent cancellations against passengers when they used African American-sounding names. Across all trips, the cancellation rate for African American sounding names was more than twice as frequent compared to white sounding names. Male passengers requesting a ride in low-density areas were more than three times as likely to have their trip canceled when they used a African American-sounding name than when they used a white-sounding name. We also find evidence that drivers took female passengers for longer, more expensive, rides in Boston. We observe that removing names from trip booking may alleviate the immediate problem but could introduce other pathways for unequal treatment of passengers."

- http://www.nber.org/papers/w22776

- Christopher Soghoian: "Your smartphone is a civil rights issue."
- https://www.ted.com/talks/ christopher_soghoian_your_smartphone_is_a_civil_rights_issue

- Predictive Policing:
- https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

Human Resources

Bott Chapter 9

What are Human Resources?

- Hiring the right people
- Keeping the balance of skills and expertise right for the work of the organisations.
- Administration relating to employment
- Complying with the law

Legal Context: HR Responsibilities

- ensuring that recruitment, selection and promotion procedures comply with anti-discrimination legislation;
- staff training and development;
- setting up and monitoring remuneration policy;
- setting up and monitoring appraisal procedures;
- administering dismissal and redundancy procedures;
- contracts of employment;
- workforce planning;
- designing and administering grievance procedures;
- being aware of new legislation affecting employment rights and advising management of what the organisation must do to comply with it;
- health and safety;
- administering consultative committees.

Recruitment and Selection

- Preparing a job description and further particulars
- Disseminating the description
- Selecting:
  - Individual Interviews
  - Panel Interview
  - References
  - Psychometric tests
  - Situational assessment
  - Task assessment
- Drive is to more" evidence-based" approaches that avoid bias (unconscious or otherwise)

Edinburgh University JD Template

- **1. Job Details**: Job title; School/Support Department; Unit (if applicable): Line manager:
- **2. Job Purpose** *(Normally no more than 2 or 3 sentences)*
- **3. Main Responsibilities** *(Normally between 4 and 10. Percentages should total at least 95% (and no more than 100%))*
- **4. Planning and Organising**
- **5. Problem Solving**
- **6. Decision Making**
- **7. Key Contacts/Relationships**
- **8. Knowledge, Skills and Experience Needed for the Job**
- **9. Dimensions**
- **10. Job Context and any other relevant information**
- **Verification** *(JDs should be agreed by the relevant manager and individual job-holder or representative. Further verification may also be specified in some cases.)*

Staff Training and Development

- Job descriptions often are derived from role descriptions.
- Role descriptions relate to a bureaucratic structure and identify the skills necessary to fulfill a particular role
- Training and development in part are oriented to fit people to more senior roles so they are eligible for promotion.
- Training can also be linked to development plans for the organisation to take account of the changing environment.

Administrative Role Profiles at Edinburgh University

- **Grade 5:** Roles at this grade will be responsible for providing or contributing to the provision of support services to an agreed quality standard or specification, within clear procedures or practices. There will be minimal day to day supervision, but clear guidance. The roles require an understanding of the allocated workload but also to react to changing priorities. Initiative is needed to handle processes and resolve problems and queries based on procedures plus experience and judgment, mainly without reference to others. May involve supervision of other staff.

Administrative Role Profiles at Edinburgh University

- **Grade 6:** Roles at this grade will be providing advice and support based on a detailed understanding of methods, systems and procedures gained through significant practical experience and/or formal training. They will exercise initiative and judgement to resolve daily problems within a range of established policies/ procedures, seeking advice on more complex issues. There is discretion to determine short-term priorities and if applicable the priorities of a team of people involved in the same type of work. Contributions include proposing and implementing improvements to current working methods

Administrative Role Profiles at Edinburgh University

- **Grade 7:** Roles at this grade will be providing advice and support to schools/departments/work units based upon a full understanding of a technical, professional or specialised field. They will plan and ensure progress within established professional procedures and university policy. They will be expected to identify gaps in information, and conduct analyses to solve/resolve problems and issues with short-term consequences. They will put forward recommendations on managing more complex situations. Individuals will be responsible for planning and organising their own work or that of a team of colleagues who may be involved in different types of work and will encounter changing priorities. There will be a need for liaison and the co-ordination of activities, across a number of subsections of a school/department/university.

Remuneration Policies and Job Evaluation

- Designing pay structures that reward individuals for work.
- Critical to the retention of key staff.
- Anti-discrimination legislations has led to an emphasis on equal pay for equal value
- Scales provide overall structure
- Job evaluation attempts to position roles/jobs in the structure:
  - Non analytical – looks at the value of the role in the company.
  - Analytical: attempts to decompose jobs into component skills.

Appraisal Schemes

- Often an annual process
- Provides a means to give feedback to employees and to encourage a forward look in terms of skills development, aspirations, …
- Oriented towards objectives (Peter Drucker, Management by Objectives).
- Review against objectives and performance measures.
- Sometimes it is difficult to fit some activities into the framework

Redundancy, dismissal and grievance procedure

- Fair dismissal:
  - Lack of capability to do the job
  - Misconduct
  - It is illegal for the employer to employ the employee
  - Redundancy
  - "Other reasons" – but many are "unfair" e.g. on grounds of discrimination, because the employee is taking legal action to enforce their rights at work, ….

Redundancy and dismissal

- Dismissal Process:
  - Written statement of why dismissal is being considered
  - Arrange a meeting where both sides can state their case
  - Following the meeting the employee is informaed of the decision.
  - Right of appeal to more senior manager
- Other issues: constructive dismissal, takeovers and outsourcing, whistleblowing

Redundancy

- Redundancy
  - Employer no longer requires people to do a particular category of job (or fewer people)
  - Employees entitled to compensation (subject to a legal minimum)
  - Often employer seeks to reduce the number of employees in a particular category
    - Traditionally selection was last-in, first-out (is this reasonable?)
    - Often voluntary redundancy is offered (do you see any issues with this?)

UK Statutory Redundancy Pay

3. Redundancy pay

You'll normally be entitled to statutory redundancy pay if you're an [employee and you've been working for your current employer for 2 years or more.](#)

You'll get:

- half a week's pay for each full year you were under 22
- one week's pay for each full year you were 22 or older, but under 41
- one and half week's pay for each full year you were 41 or older
- Length of service is capped at 20 years.
- If you were made redundant on or after 6 April 2017, your weekly pay is capped at £489 and the maximum statutory redundancy pay you can get is £14,670. If you were made redundant before 6 April 2017, these amounts will be lower.

Redundancy pay (including any severance pay) under £30,000 isn't taxable.

Contracts of Employment

- In most modern economies employees are required to have contracts (whether or not they are written)

- Employees should understand their conditions of employment.

- HR staff oversee the signing and record keeping around contracts.

Human Resource Planning

- HR departments often get involved in resource planning:
  - Characterizing the skills of the current workforce
  - Characterizing the current workload and how effectively the workforce meets that workload
  - Forecasting likely increases in workload and the pattern of workload
  - Forecasting staff losses and gains
  - Predicting the effects of takeovers etc on HR.

Summary

- Human resources consider all aspects of getting the right people to do the work of the organisation.
- This includes:
  - Good processes for finding and hiring the right people
  - Good processes to handle issues for individuals during employment
  - Good processes to manage the balance of human resource against the organizational workload.

Edinburgh University Mission

Edinburgh University HR Work Themes

- **Developing and implementing simple and consistent processes and systems** – in line with the University's Service Excellence Programme, making better use of technology and digital solutions, and developing and implementing common standardised processes.

- **Helping to create a flexible organisation** – developing contractual arrangements to support flexible working patterns including overseas working, remote working, joint appointments with external partners, matrix reporting structures and secondments.

- **Supporting the evolution of the workforce** – developing and delivering internationally and locally focused attraction and recruitment strategies, succession planning and talent management, technical and personal skills development (e.g. digital skills, leadership skills) and change management.

- **Making staff engagement and wellbeing a reality** – supporting employee engagement, career development, reward and recognition and promoting equality, diversity and inclusion, and physical, mental, emotional and financial wellbeing.

Edinburgh University HR Work Practice

- **Simplification** – ensuring that policies and processes are easy to access, easy to use and easy to understand

- **Facilitation** – providing HR support that is focused on understanding business problems and providing practical solutions

- **Anticipation** – adopting a planned approach to managing projects, anticipating and responding to the changing needs of customers and providing solutions that are fit for the future.

Edinburgh University HR Activities

- provide advice and guidance to managers to help them carry out their management roles effectively
- provide advice and guidance to staff on employment policies and processes
- work in partnership with our recognised Trade Unions
- maintain and manage systems and processes that support the employee lifecycle
- ensure compliance with employment legislation and statutory reporting obligations

(Adapted from Management School Talk)

WORKING IN TEAMS (MAY BE SDP RELEVANT)

Belbin Team Roles

Session Guide
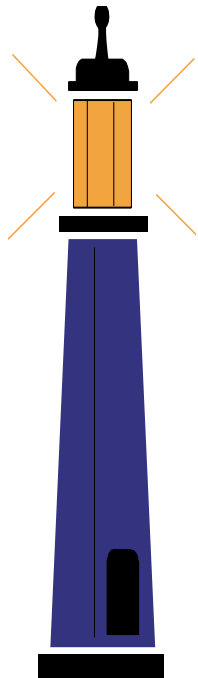
Belbin team types

Implications / issues

Action planning

Context

Research by Meredith Belbin

Effective Teams

Key Roles for Success

Situation Dependent
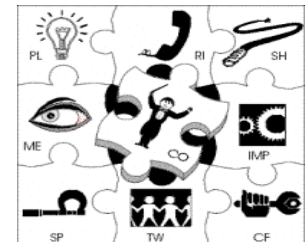
9 Roles

Contribution to Team

Allowable Weaknesses

All of equal value

Dropped Points

Leadership Roles

Shaper

Co-ordinator
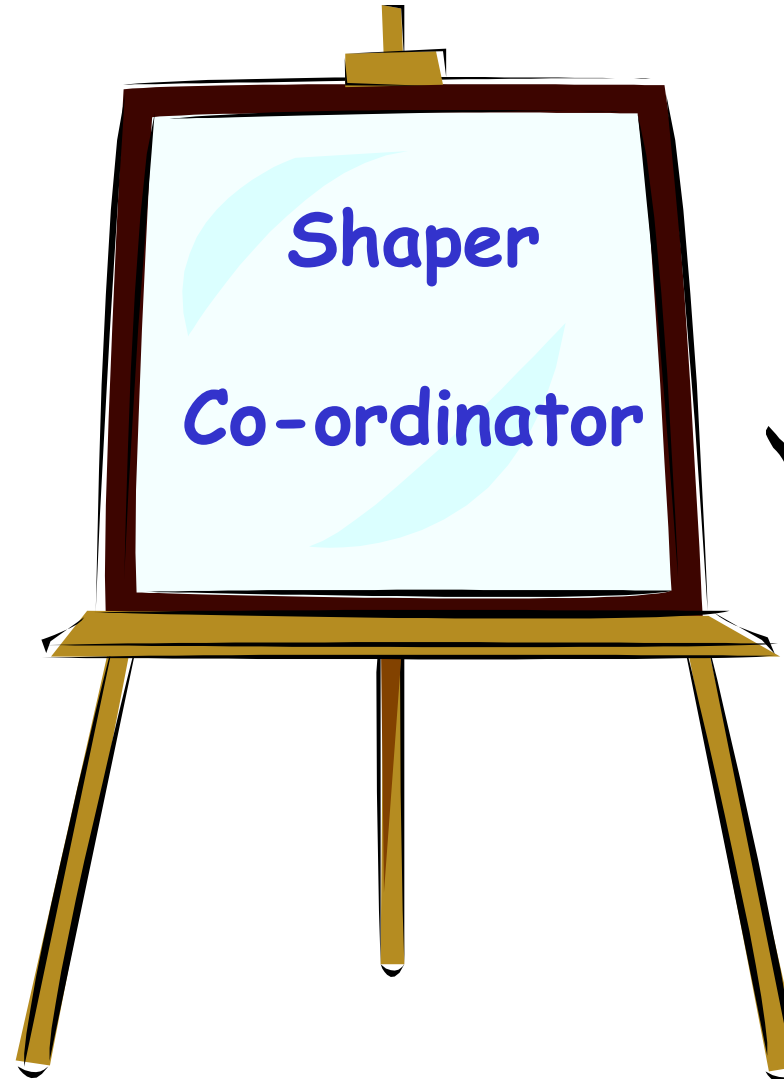
Creative Roles

Plant
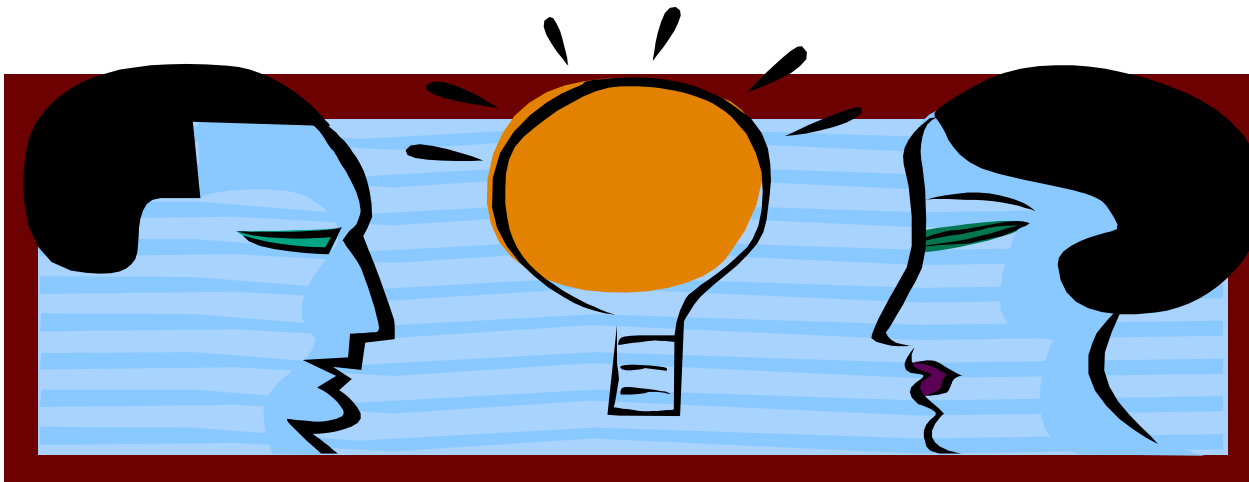
Resource Investigator

……the other Roles

Monitor Evaluator

Implementer

Completer Finisher

Team Worker

Specialist

Belbin Roles

Descriptions of Belbin roles

Name	Symbol	Behavioral description	Typical features	Positive qualities	Allowable weaknesses
Chairman	CH	Guiding and controlling leader, knows the members' abilities well	Calm, self-confident, controlled	A capacity for treating and welcoming all potential contributors on their merits and without prejudice. Strong sense of objectiveness	No more than ordinary in terms of intellect or creative ability
Shaper	SH	Demanding, coercing, confrontational leader, pushes for members to excel	Highly strung	Drive and a readiness to challenge inertia, ineffectiveness, complacency or self-deception	Proneness to provocation, irritation and impatience
Plant	PL	Innovator and problem solver, the "idea" member	Individualistic, serious-minded, unorthodox	Genius, imagination, intellect, knowledge	Up in the clouds, inclined to disregard practical details or protocol

Belbin Roles

Resource Investigator	RI	Contact person for resources external to the team, brings resources into the team	Extroverted, en-thusiastic, curious, communicative	A capacity for contacting people and exploring anything new. An ability to respond to challenge	Liable to lose interest once the initial fascination has passed
Monitor-Evaluator	ME	Analyzes, evaluates proposed solutions and choices	Sober, unemotional, prudent	Judgement, discretion, hard-headedness	Lacks inspiration or the ability to motivate others
Company Worker	CW	Implements agreed upon plans	Conservative, dutiful, predictable	Organizing ability, practical common sense, hard-working, self-discipline	Lack of flexibility, un-responsiveness to unproven ideas

Belbin Roles

Team Worker	TW	Facilitates team functions, mediates issues within the team	Socially oriented, mild, sensitive	Ability to respond to people and to situations, and to promote team spirit	Indecisiveness at moments of crisis
Completer-Finisher	CF	Focuses on details and meeting deadlines	Painstaking, orderly, conscientious, anxious	A capacity for follow-through, perfectionism	A tendency to worry about small things, a reluctance to "let go"

33

Belbin research findings

Roles can equally be applied to non-managers
Fisher, Hunter & Macrosson
Journal of Managerial Psychology, Vol.17 No.1, (2002)

Balanced teams perform better than biased teams
Shapers vs. Balanced
Pritchard & Stanton
Journal of Management Development, Vol 18, No.8, (1999)

No correlation between salary/status and team role
Dulewicz
Journal of Occupational & Organisational Psychology
Vol 68, Issue 2 (1995)
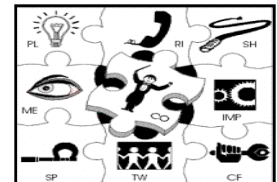
Belbin in UK Managers

1441 male / 355 female

Predicting team roles from established personality profiles

High validity suggested

Findings:

1. Suggested surplus of co-coordinators and resource investigators

2. Suggested dearth of *Completers, Monitor Evaluators , Plants and Shapers*......relatively few who have this as a primary or secondary role.

3. Lack of the balanced teams in UK industry

Fisher, Hunter & Macrosson
Personnel Review, Vol.29 No.2, (2000)
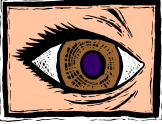
Belbin Team Types

Resource Investigator → **Ideas** ← **Plant**

Co-ordinator → **Optimal Solution** ← **Monitor Evaluator**

Shaper → **Clear goals, objectives** → **Specialist**

Implementer → **Work** ← **Completer finisher**

↓

Success

← **Team Worker**

Belbin and Career Management

Team Role	Career Planning	Job Search	Written Application	Selection Process	Pro-active Follow-up
Plant	Strong on ideas May lack focus	Research strong Networking weak	Potentially unorthodox Insensitive to company needs	May lack focus May compete with others Insensitive to company needs	Feedback seen as irrelevant Learning minimised
Resource Investigator	Strong on ideas	Networking strong May become disillusioned	Uncomfortable with medium	Thrives on group activities	OK
Co-ordinator	OK	OK	Finds self-marketing difficult	May undersell self Prefers group activities	Strength

Belbin and Career Management

Team Role	Career Planning	Job Search	Written Application	Selection Process	Pro-active Follow-up
Shaper	Action focus-less emphasis on planning May set unrealistic goals	High expectations and self belief	May oversell achievements	May oversell self May compete with others	Feedback seen as irrelevant Learning minimised
Monitor Evaluator	Tends to over-analyse May be indecisive	May be indecisive	Prone to too much detail	Dislikes deadlines May be indecisive	Tends to over-analyse Own harshest critic
Team Worker	May be indecisive	OK	Finds self-marketing difficult	Prefers group activities May undersell self	Accepts feedback

Belbin and Career Management

Team Role	Career Planning	Job Search	Written Application	Selection Process	Pro-active Follow-up
Implementer	May be inflexible and lack motivation	OK	OK	May lack creativity	OK
Completer Finisher	May be inflexible and indecisive	May be indecisive	Prone to too much detail	Avoids leadership High anxiety May be indecisive	Tends to over-analyse
Specialist	Narrow perspective may limit opportunities	May not consider wider options	Prone to too much detail and jargon	May constrain input to specialism	May underestimate relevance

Summary

✓ Insight into our own team role allows us to work on our strengths and weaknesses

✓ A knowledge of team roles helps us build balanced teams

✓ A knowledge of team roles helps us develop more effective teams

> "When he took time to help the man up the mountain, lo, he scaled it himself."
> Tibetan Proverb

Computer Misuse Act 1990

Anti-hacking legislation

Background

- No laws specifically to deal with computer crime prior to 1990

- Other laws tried instead

- Examples.

  - Cox v Riley 1986 (Criminal Damage Act 1971)
  - R. v Whitely 1990 (Criminal Damage Act 1971)
  - R. v Gold and Another (Forgery and Counterfeiting Act 1981)

Background 2

- The case of *R. v Gold and Another* was highly publicised

- Defendant released on appeal

- Lead to Law Commission produced report
    - Report No.186, Computer Misuse

- Michael Colvin's (MP) Private Member's Bill

- This became the Computer Misuse Act 1990

Problems

- Original bill specifically aimed at hackers
- Many amendments during passage through parliament
- Eventual legislation very broad based, lost much of the original intent

Offences

- The Act specifies 3 offences
- In summary these are:-
    - Unauthorised Access
    - Unauthorised access with intent to commit another offence
    - Unauthorised modification of data

Penalties 1

- Unauthorised Access is called a *summary offence* and penalties are limited to
  - 6 months imprisonment

  and/or

  - a maximum fine of £5000

Penalties 2

- The other two offences
    - Unauthorised access with intent…
    - Unauthorised modification …
- Are more serious and carry jail terms of up to 5 years and unlimited fines

Examples 1

Scenario 1

- A student hacks into a college database to impress his friends - unauthorised access

- Later he decide to go in again, to alter his grades, but cannot find the correct file - unauthorised access with intent...

- A week later he succeeds and alters his grades - unauthorised modification of data

Examples 2

Scenario 2

- An employee who is about to made redundant finds the Managing Director's password; logs into the computer system using this and looks at some confidential files- unauthorised access

- Having received his redundancy notice he goes back in to try and cause some damage but fails to do so - unauthorised access with intent...

- After asking a friend, he finds out how to delete files and wipes the main customer database - unauthorised modification

Problems

- While there has been a rise in hacking
    - more computers/Internet gives greater access

- Prosecution are rare and punishments small
    - Examples
        - Defendant causes firm to lose £36,000 - Fined £1,650; conditional discharge
        - Defendant destroys £30,000 worth of data - Fined £3000; 140 hours community service

Reasons

- **Very complex**
  - Offences difficult to prove
  - Evidence difficult to collect - firms do not co-operate with police
  - Firms embarrassed by hacking - particularly banks
  - Employees often simply sacked/demoted
  - Police lack expertise; time; money
  - Offence perceived as 'soft crime' no one injured/hurt

The Bedworth case

- This case in 1991 caused great concern and it was suggested that further prosecutions under the act would be unlikely to succeed
  - Defendant (and others) hacked into a variety of systems and caused damage
  - Defence stated that defendant 'addicted to computers' so could not help hacking
  - Not guilty verdict returned by jury

Current situation

- Hacking has increased both at hobby and professional levels

- A few high profile cases

- Offenders often in other countries with no equivalent legislation

- Some 'international task forces' set up but no real progress

- Current estimated costs of hacking - £5 billion per year world-wide

The End

CS38010

Profit and Loss

	1	2	3	4	5	6
Sales	10K					
Costs	8K					
Profit	2K					
Accum Profit	2k					

Profit and Loss

	1	2	3	4	5	6
Sales	10K	12K				
Costs	8K	9K				
Profit	2K	3K				
Accum Profit	2k	5K				

Profit and Loss

	1	2	3	4	5	6
Sales	10K	12K	12K			
Costs	8K	9K	9K			
Profit	2K	3K	3K			
Accum Profit	2k	5K	8K			

4

Profit and Loss

	1	2	3	4	5	6
Sales	10K	12K	12K	13k		
Costs	8K	9K	9K	10K		
Profit	2K	3K	3K	3K		
Accum Profit	2k	5K	8K	11k		

Profit and Loss

	1	2	3	4	5	6
Sales	10K	12K	12K	13k	14K	
Costs	8K	9K	9K	10K	10K	
Profit	2K	3K	3K	3K	4K	
Accum Profit	2k	5K	8K	11k	15K	

6

Profit and Loss

	1	2	3	4	5	6
Sales	10K	12K	12K	13k	14K	14K
Costs	8K	9K	9K	10K	10K	10
Profit	2K	3K	3K	3K	4K	4K
Accum Profit	2k	5K	8K	11k	15K	19K

Payment Cycle

- Send Invoice end of Month
- Receive Money 1 to 2 months later
- Therefore up to 3 months salaries, rents, bills to pay.

- NEED CASH!!!

Cashflow
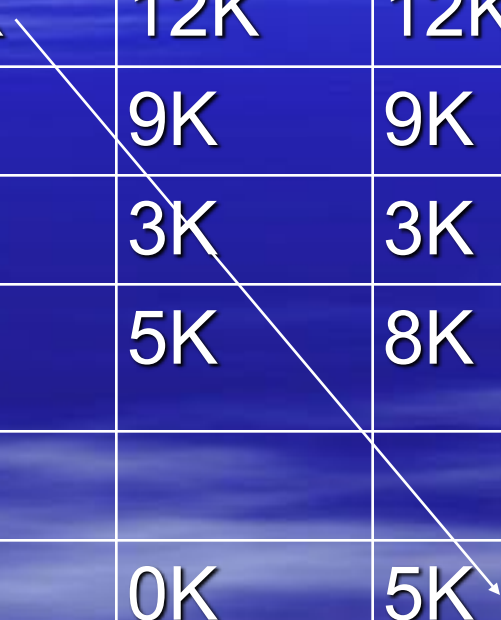
	1	2	3	4	5	6
Sales	10K	12K	12K	13k	14K	14K
Costs	8K	9K	9K	10K	10K	10
Profit	2K	3K	3K	3K	4K	4K
Accum Profit	2k	5K	8K	11k	15K	19K
Cash in	0K					
Cash Out	-8K					
Balance	-8K					

Cashflow

	1	2	3	4	5	6
Sales	10K	12K	12K	13k	14K	14K
Costs	8K	9K	9K	10K	10K	10
Profit	2K	3K	3K	3K	4K	4K
Accum Profit	2k	5K	8K	11k	15K	19K
Cash in	0K	0K				
Cash Out	-8K	-9K				
Balance	-8K	-17K				

Cashflow

	1	2	3	4	5	6
Sales	10K	12K	12K	13k	14K	14K
Costs	8K	9K	9K	10K	10K	10
Profit	2K	3K	3K	3K	4K	4K
Accum Profit	2k	5K	8K	11k	15K	19K
Cash in	0K	0K	5K			
Cash Out	-8K	-9K	-9K			
Balance	-8K	-17K	-21			

Cashflow

	1	2	3	4	5	6
Sales	10K	12K	12K	13k	14K	14K
Costs	8K	9K	9K	10K	10K	10
Profit	2K	3K	3K	3K	4K	4K
Accum Profit	2k	5K	8K	11k	15K	19K
Cash in	0K	0K	5K	11K		
Cash Out	-8K	-9K	-9K	-10K		
Balance	-8K	-17K	-21K	-20K		

Cashflow

	1	2	3	4	5	6
Sales	10K	12K	12K	13k	14K	14K
Costs	8K	9K	9K	10K	10K	10K
Profit	2K	3K	3K	3K	4K	4K
Accum Profit	2k	5K	8K	11k	15K	19K
Cash in	0K	0K	5K	11K	12K	
Cash Out	-8K	-9K	-9K	-10K	-10K	
Balance	-8K	-17K	-21K	-20K	-18K	

13

Cashflow

	1	2	3	4	5	6
Sales	10K	12K	12K	13k	14K	14K
Costs	8K	9K	9K	10K	10K	10K
Profit	2K	3K	3K	3K	4K	4K
Accum Profit	2k	5K	8K	11k	15K	19K
Cash in	0K	0K	5K	11K	12K	13K
Cash Out	-8K	-9K	-9K	-10K	-10K	-10K
Balance	-8K	-17K	-21K	-20K	-18K	-15K

14

Types of Software House

- **Body Shopping Services**
  - Needs a few months working capital
- **Product Developer**
  - Needs perhaps a year or more development funds
- **Bespoke Software**
  - Could use advances from customer to help cash flow

Getting the Money

- Business Plan
  - Description of Business
  - Technical feasibility
  - Founders expertise
  - Market size
  - Competition
  - Financial prediction

- More later in a further lecture

Sources of Funds

- Grants
- Loans
- Equity

Grants

- Money *given* to a company
  - Government (British and Welsh Government)
  - European (Objective 1 & Convergence Fund))
  - Charities (Cancer Research)
  - Rent/Rate free buildings (Local government)
- Restrictions can be
  - Fund matching
  - Only on certain projects
  - On Certain costs

Loans

- Money *lent* to a company
  - Interest payable on it
  - Borrower wants to get all money back
    - On liquidation, paid by sale of assets and cash
  - Personal Guarantees
    - Directors risk homes
  - Match Funding
    - 50/50 Bank and Company

Loans (2)

- Loan types
  - Overdrafts
    - Flexible
    - Interest only on overdrawn amount
    - Bank can withdraw the facility at very short notice (and they do!!)
  - Short/Long Term term loans
    - Fixed Interest
    - Cannot be withdrawn if payments met
  - Soft Loans
    - Government sponsored
    - Less onerous terms

Equity Capital

- Money *paid* to company for a *share* of that company

- Risks versus rewards
  - Possible greater reward for shareholders
    - Share price rise
    - Dividends

The Structure of Organisations & Finance

Costs and Prices

Costs and Prices

- What's the difference

Costs and Pricing

🔴 Costs
- What it costs YOU to deliver a product or service

🔴 Price
- Is what your CUSTOMER pays

Costs

- Purchase costs
  - Raw materials
  - Equipment Costs
- Costs of Finance
  - Interest Payable or Lost
- Direct Labour Costs
  - Salaries
  - Pensions
- Overhead Costs
  - Premises, Admin, Sales & Marketing
  - Not attributable to projects

Costs of Running a Car

- Cost £10,000
- Run for 3 years
- Sell for £4,200
- 10,000 miles per year

Cost of Running a Car …..

Fixed Costs:		
Depreciation	5800	
Loss of Interest	927	
Car Tax	475	
Insurance	1500	
Total Fixed Costs	8702	29p/mile
Variable Costs:		
Petrol	3300	
Servicing	300	
Total Fixed	3600	
TOTAL COST	12302	41p/mile

No Inflation

Costs......

🔴 Fixed
- – Premises
- – Administration
- – Sales & Marketing
- – Costs of Finance

🔴 Variable
- – Raw Materials
- – Direct Labour Costs

Fixed & Variable Costs

🔴 Production Units Can Have Fixed Costs

- Independent of Sales

- Magazine Publishing

- Toy Manufactures

- Software Development

Depreciation

- Need to know value of Equipment and Stock
- Too costly to revalue every Item
- Simplified:
  - Straight Line
  - Reducing Balance

- *Must be Consistent and Used & Declared in Annual Accounts*

Straight Line Depreciation

Year	Depreciation	End Year Value
1	2000	8000
2	2000	6000
3	2000	4000
4	2000	2000

Reducing Balance Depreciation

Year	Depreciation	End Year Value
1	3000	7000
2	2100	4900
3	1470	3430
4	1029	2401

Reducing Balance........

- Need to Identify Classes of Equipment
- Computers – High depreciation rate
- Buildings - Low rate
- Cars – Medium rate
- Furniture – Low rate

Labour Costs

- Salary plus on costs:
  - National Insurance
  - Pensions
- Persons Day rate
  - Statutory & Ordinary Holidays
  - Sickness
  - Training
  - Idle time
  - Unchargeable Time

Staff Costs

- Total Work Days 260
- Junior Staff – 220 Chargeable days
- Senior Staff - 160 Chargeable days

- Junior on £20,000
  - Cost £24,000 (No overheads)
  - Overheads £24,400
  - Cost per day = £220 per day

Overhead Costs

🔴 Not Attributable to Particular project
- – Building Costs
- – Administration
  - •Personnel
  - •Finance
  - •Sales & Marketing
  - •Support

🔴 Fixed Costs and are very Real!!

🔴 Computer Industry
- – 100% Small Company
- – 200 – 250% Large Company

Pricing

Pricing in the Computer Industry

- Cost Plus Services
- Fixed price
- Products

Cost Plus – Project Work

- Agree with Client your Costs per day
  - Usually on Direct Labour
  - Overhead
- Agree Profit margin
- "Body shopping"
- Unsuitable today for projects but used to supply skills/experience to customer projects

Fixed price – Project Work

- Total of:
  - Direct Labour
  - Bought in Items
  - Indirects
- Profit added
- Used in Competitive Tendering
- Risks versus Profit

Project Costings for F P jobs

Companies may differ in the way they do this but basically the same idea

Labour Costs

Arrange staff into levels, grades etc

Work out average salary in each grade

Work out average daily salary in each grade

Labour Costs cont'd

Add to daily amount a sum of money to cover the overheads

Therefore if all fee paying staff work then we can cover our costs

Add it up with more amounts!!

Add contingency

Add Hardware

Add Mark up

Add Profit

Arrive at the final "Price"

Software Product Pricing

- Marginal Costs Very Low
  - Manual, Box and CD Rom < £10.00

- Large Development Costs

- Amortised over time

- Sales proportional to marketing

- Sales fall with increasing price

Customer Expectations

Price	Nature (Low to High)
Free	Shareware etc. Some great products (Winzip)
£20	Buyer's Risk – Internet Sales
£100 -£500	High volume - Real Software – Microsoft, Adobe
£10,000	Real product – low volume – Bugs and Support
£100,000	On the drawing board!!

Support and other Issues

- Large percentage of income
  - 10% - 25% of turnover
  - Sage, Microsoft
- Support & Updates
- Must be Real and Valuable

- Annual Licence fee charges
- Per use Charges
- Application Service Providers

CS38010

P/L Costs Overheads

- Wages
- NI
- Rent
- Rates – Business & Water
- Gas & Electricity
- Telephone, ISP
- Postage, Printing, Stationary
- Advertising
- Insurance

P/L Costs ……..

- Repairs & Maintenance
- Interest Payments
- Bank Charges
- Depreciation
- Travel
- Legal
- Subscriptions and Periodicals

Sales And Income

- Invoice sales
- Cash Sales
- Interest on deposit

Cash In – Not Sales

- Equity
- Bank Loan/Mortgage
- VAT

- These DO NOT appear in profit/loss

Capital Equipment

- Capital Equipment does not appear in the P/L

- It is taken from the cashflow and the depreciation is treated as a cost in the P/L

Balance Sheet

- Snap Shot on a particular date
- How much are you worth?
  - Assets
    - Fixed Asset
    - Liquid (Current) Assets
- How much do you owe?
  - Tax
  - VAT
  - Creditors
  - Bank Loans
  - Shareholders

Balance Sheet

- Assets = Liabilities +Shareholders Equity
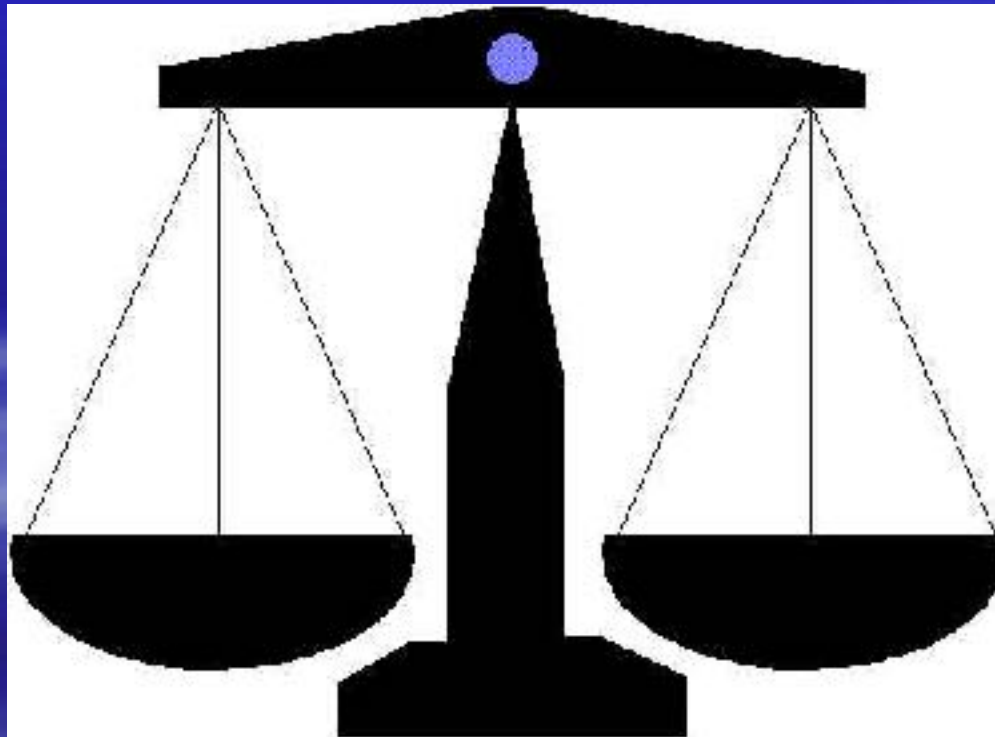
Start up

- Shareholders raise £50,000
- Cash goes into bank

- Assets
  – Cash on hand £50,000

- Liabilities + Sharehldrs
  – £0   +£50,000

Trading for a while

- Sales £10,000 (invoiced)
- Vat £1750
- Purchases £2,000

- Assets
  - Receivables   £11750
  - Cash on hand £48,000
  - Computers   £2,000
  - Total   £61,750

- Liabilities & Sharehldrs
  - Profit   £10,000
  - Vat   £1,750
  - Shares   £50,000
  - Total   £61,750

Balance Sheet

- **Assets**
  - Current
    - Cash
    - Accounts Receivable
    - Inventory
  - Long Term
    - Fixed or Tangible
      - Buildings, Furniture, Plant & Machinery
    - Intangible
      - Name & Goodwill
      - Patents
      - Website

Balance Sheet

- Liabilities
  - Current Liabilities
    - Accounts Payable
    - Loan Payment Payable
    - VAT
    - Inland Revenue
  - Long Term Debt
    - Remainder of Loan

Balance Sheet

- Shareholder Equity
  - Shareholdings
  - Retained profit

Equation

- Assets = Liabilities + Shareholders Equity

Start of Business

- Sell shares for £50,000 on day
- Therefore balance sheet reads
- Assets = £50K
- Liabilities + £0
- Shareholders Equity = £50K

- £50K = £0 + £50K

P/L & Cashflow

	1	2	3	4	5	6
Sales	10K	12K	12K	13k	14K	14K
Costs	-8K	-9K	-9K	-10K	-10K	-10K
Profit	2K	3K	3K	3K	4K	4K
Accum Profit	2k	5K	8K	11k	15K	19K
Cash in	0K	0K	5K	11K	12K	13K
Cash Out	-8K	-9K	-9K	-10K	-10K	-10K
Balance	-8K	-17K	-21K	-20K	-18K	-15K

P/L & Cashflow now looks like

	1	2	3	4	5	6
Sales	10K					
Costs	-8K					
Profit	2K					
Accum Profit	2k					
Cash in	£50K					
Cash Out	-£8K					
Cash on Hand	£42K					

Balance sheet month end 1

- Assets
  £10K in receivables
  £42K in the bank

  Liabilities
  Shareholders Equity =
  £50K Shares
  £2K profit

- £10K + £42K = £50K + £2K

Purchases Month 2

- During Month 2 we purchase £22K of hardware

P/L & Cashflow

	1	2				
Sales	10K	12K				
Costs	-8K	-9K				
Profit	2K	3K				
Accum Profit	2k	5K				
Cash in	50K	0K				
Cash Out	-8K	-31K	(9K costs and 22K equipment)			
Cash on	42K	11K				

Balance sheet Month 2

- **Assets**
  Receivables = £22K Outstanding invoices
  Assets = £22k New equipment (no depreciation)
  Cash = £11K

- **Liabilities**
  £0

- **Shareholders equity**
  Shares = £50K
  Profit = £5K

Month 3

- Money starts to come in
- Depreciation started

P/L & Cashflow

	1	2	3			
Sales	10K	12K	12K			
Costs	-8K	-9K	-9K			
Deprecation			-1K			
Profit	2K	3K	2K			
Accum Profit	2k	5K	7K			
Cash in	50K	0K	5K			
Cash Out	-8K	-31K	-9K			
Cash on Hand	42K	11K	7K			

Balance Sheet Month 3

- Assets
  Invoiced £34K, received £5K.
  Therefore:
  Receivables = £29K
  Assets = £21K
  Cash = £7K

- Liabilities
  £0

- Shareholders Equity
  £50K Shares
  £7K Profit

Balance Sheet

- (29+21+7)K = (50+7)K

Receivables

Assets

Cash

Profit

Shares

Remember 1

- Try this by purchasing items on credit to create liabilities
  - You put how much you owe on the liabilities side and the new item into your assets.
  - This balances.
- When you pay it off you lose the liability on one side and the cash from your asset side.

Remember 2

- Reduce the profit (shareholders equity) by the depreciation to date, balances with loss of same amount on the assets side of the equation.

- Balance sheets BALANCE.

- Balance sheets run vertically

Example 2

- Shares = £50,000
- Salaries = £8,000 per month
- Sales £15,000 per month
- Equipment = £12,500 Month 1 using cash
- Fixed Costs £4,000

1. Raise capital	P/L Account: £0
Cashflow: £50,000	Balance Sheet: Assets = Liabilities + Shareholders Equity £50,000 = 0 +£50,000

2. Purchase equipment for £12,500 using cash	P/L Account: £0
Cashflow: £37,500	Balance Sheet: Assets = Liabilities + Shareholders Equity £37,500 + £12,500 = 0 + £50,000 Cash Equipment

3. Sales Invoices sent Labour fees = £15,000	**P/L Account:** £15,000
Cashflow: £37,500	**Balance Sheet:** Assets = Liabilities + Shareholders Equity £37,500 + £12,500 + £15,000 Cash Equipment Invoices = £0 + (£50,000 + £15,000) Liabilities

4. Pay the wages and the fixed costs	P/L Account:
Salaries £8,000	£15,000 - £12,000
Fixed costs £4,000 Total £12,000	= £3,000
Cashflow: £37,500 - £12,000 = £25,500	**Balance Sheet:** Assets = Liabilities + Shareholders Equity £25,500 + £12,500 + £15,000 Cash Equipment Invoices = £0 + (£50,000 + £3,000) Liabilities

5 Month 2 receive all cash (unexpectantly) Cash in = £15,000	P/L Account: £3,000
Cashflow: £25,500 + £15,000 =£40,500	Balance Sheet: Assets = Liabilities + Shareholders Equity £25,500 + £12,500 + £15,000 Cash Equipment New cash = £0 + (£50,000 + £3,000) Liabilities

6. Purchase £16,500 of equipment on 30 days credit	P/L Account: £3,000
Cashflow: £40,500	Balance Sheet: Assets = Liabilities + Shareholders Equity £40,500 + £12,500 + £16,500 Cash Equip + new equip now = £16,500 + (£50,000 + £3,000) Liabilities + Shareholders

7. Pay: Equipment bill £16,500 Salaries £8,000	**P/L Account:** £3,000 last month £3,000 this month
Fixed £4,000 Invoice fees £15,000	
Cashflow: £40,500 - £28,500 = £12,000	**Balance Sheet:** Assets = Liabilities + Shareholders Equity £12,000 + £29,000 + £15,000 Cash Equip Invoices = £0 + (£50,000 + £6,000) Liabilities + Shareholders

Discrimination

Professional Issues

22%
SAID THEY WERE
TREATED DIFFERENTLY

REASONS WHY THEY FELT THEY WERE
TREATED DIFFERENTLY

RACE/ETHNICITY	35%
OTHER FACTOR	30%
NATIONAL ORIGIN	17%
AGE	16%
SEX/PREGNANCY	15%
GENDER	10%
RELIGION	5%
DISABILITY	5%
MEDICAL CONDITION	4%
MARITAL STATUS	3%
SEXUAL ORIENTATION	3%

1. Types of discrimination ('protected characteristics')

It is against the law to discriminate against anyone because of:

- age
- being or becoming a transsexual person
- being married or in a civil partnership
- being pregnant or on maternity leave
- disability
- race including colour, nationality, ethnic or national origin
- religion, belief or lack of religion/belief
- sex
- sexual orientation

You're protected from discrimination:

- at work
- in education
- as a consumer
- when using public services
- when buying or renting property
- as a member or guest of a private club or association

You're legally protected from discrimination by the Equality Act 2010.

You're also protected from discrimination if:

- you're associated with someone who has a protected characteristic, eg a family member or friend
- you've complained about discrimination or supported someone else's claim

The Equality Act 2010

The Equality Act - Introduction

- Single largest piece of anti-discrimination legislation the UK has known.
- Harmonises multiple pieces of primary and secondary legislation.

Action against discrimination

You can do something voluntarily to help people with a protected characteristic. This is called 'positive action'.

Taking positive action is legal if people with a protected characteristic:

- are at a disadvantage
- have particular needs
- are under-represented in an activity or type of work

2. How you can be discriminated against

Discrimination can come in one of the following forms:

- direct discrimination -
  treating someone with a protected characteristic less favourably than others
- indirect discrimination -
  putting rules or arrangements in place that apply to everyone, but that put someone with a protected characteristic at an unfair disadvantage
- harassment -
  unwanted behaviour linked to a protected characteristic that violates someone's dignity or creates an offensive environment for them
- victimisation -
  treating someone unfairly because they've complained about discrimination or harassment

It can be lawful to have specific rules or arrangements in place, as long as they can be justified.

3. Discrimination at work

The law protects you against discrimination at work, including:

- dismissal
- employment terms and conditions
- pay and benefits
- promotion and transfer opportunities
- training
- recruitment
- redundancy

It can be lawful to have specific rules or arrangements in place, as long as they can be justified.

3. Discrimination at work

The law protects you against discrimination at work, including:

- dismissal
- employment terms and conditions
- pay and benefits
- promotion and transfer opportunities
- training
- recruitment
- redundancy

Some forms of discrimination are only allowed if they're needed for the way the organisation works, eg:

- a Roman Catholic school restricting applications for admission of pupils to Catholics only
- employing only women in a health centre for Muslim women

Disability

If you're disabled you have the same rights as other workers. Employers should also make 'reasonable adjustments' to help disabled employees and job-applicants with:

- application forms, eg providing forms in Braille, audio formats
- aptitude tests, eg giving extra time to complete the tests
- dismissal or redundancy
- discipline and grievances
- interview arrangements, eg wheelchair access, communicator support
- making sure the workplace has the right facilities and equipment for disabled workers or someone offered a job
- promotion, transfer and training opportunities
- terms of employment, including pay
- work-related benefits such as access to recreation or refreshment facilities

Definition:

Over the last few decades' new research from the fields of neuroscience and social psychology has shed light onto the working of the human brain and the concept of unconscious bias.
Unconscious biases are simply our unintentional people preferences, which are created and maintained by the way our brains work, to sort data quickly and are influenced by our upbringing, the media and our life experiences.

IT can play a major role in alleviating the effects of disability and allow independent living by enabling

- The blind and vision impaired to see
- The deaf and hard of hearing to listen
- The mute to speak
- The physically disabled to control their environment
- Those with cognitive impairments to understand better

In a world of 'digital by default'
knowledge of disability, and of the beneficial influence of IT,
should be part of the background knowledge of all IT professionals.

4. What you can do

If you think you've been unfairly discriminated against you can:

- complain directly to the person or organisation
- use someone else to help you sort it out (called 'mediation' or 'alternative dispute resolution')
- make a claim in a court or tribunal

Contact the Equality Advisory Support Service for help and advice.

Discrimination at work

Employees should talk to their employer first to try and sort out the problem informally. You may also want to read about workplace disputes.

If things can't be sorted out informally, talk to Acas, Citizens Advice or a trade union representative.

You might be able to take a claim to an employment tribunal for discrimination.

Employers: preventing discrimination

1. Overview

It is against the law to treat someone less favourably than someone else because of a personal characteristic, eg religion, gender or age.

Discrimination can include:

- not hiring someone
- selecting a particular person for redundancy
- paying someone less than another worker without good reason

You can discriminate against someone even if you don't intend to. For example, you can discriminate indirectly by offering working conditions or rules that disadvantage one group of people more than another.

2. Discrimination during recruitment

Discrimination in job adverts

You must not state or imply in a job advert that you'll discriminate against anyone.
This includes saying that you aren't able to cater for workers with a disability.

Only use phrases like 'recent graduate' or 'highly experienced' when these are actual requirements of the job. Otherwise you could discriminate against younger or older people who might not have had the opportunity to get qualifications.

Where you advertise might cause indirect discrimination - for example, advertising only in men's magazines.

Questions you can't ask when recruiting

You must not ask candidates about 'protected characteristics' or whether they:

- are married, single or in a civil partnership
- have children or plan to have children

Asking about health or disability

You can only ask about health or disability if:

- there are necessary requirements of the job that can't be met with reasonable adjustments
- you're finding out if someone needs help to take part in a selection test or interview
- you're using 'positive action' to recruit a disabled person

Asking for a date of birth

You can only ask for someone's date of birth on an application form if they must be a certain age to do the job, eg selling alcohol.

You can ask someone their date of birth on a separate equality monitoring form. You shouldn't let the person selecting or interviewing candidates see this form.

Spent criminal convictions

Applicants don't have to tell you about [criminal convictions that are spent](). You must treat the applicant as if the conviction has not happened, and cannot refuse to employ the person because of their conviction.

There are some areas of employment that are exempt from this rule, eg schools.

Trade union membership

You must not use membership of a trade union as a factor in deciding whether to employ someone. This includes:

- not employing someone because they're a member of a trade union
- insisting someone joins a trade union before you'll employ them

Employing people with protected characteristics

You can choose a candidate who has a protected characteristic over one who doesn't if they're both suitable for the job and you think that people with that characteristic:

- are underrepresented in the workforce, profession or industry
- suffer a disadvantage connected to that characteristic
  (eg people from a certain ethnic group are not often given jobs in your sector)

You can only do this if you're trying to address the under-representation or disadvantage for that particular characteristic. You must make decisions on a case by case basis and not because of a certain policy.

You can't choose a candidate who isn't as suitable for the job just because they have a protected characteristic.

Favouring disabled candidates

When a disabled person and a non-disabled person both meet the job requirements, you can treat the disabled person more favourably.

Which of these are under-represented in IT?

3. Discrimination during employment

You must not discriminate against your employees. This could be done by, for example:

- introducing measures that discriminate between workers, eg a benefit for married employees that's not available for people in a civil partnership
- paying men and women different amounts (this includes benefits, eg company cars) when they're doing work of equal value
- selecting someone for redundancy because they have a protected characteristic
- failing to make reasonable adjustments for a disabled worker
- firing someone for making an allegation of discrimination
- firing someone because they're a union member
- unfairly rejecting a request for flexible working from a new parent

This includes self-employed people on a contract for you.

Training and promotion can't just happen because of an employee's age or the time they've worked for you.

You're allowed to ask employees about their future career plans, including retirement. But you can't just choose older workers for discussions about retirement. Such talks should be part of general discussions about each worker's career development.

Employment tribunals

An employee who thinks they've been discriminated against may raise a grievance or take their case to an employment tribunal.

You're responsible for discrimination carried out by your employees unless you can show you've done everything you reasonably could to prevent or stop it.

Employing family members

If you hire members of your family you must:

- avoid special treatment in terms of pay, promotion and working conditions
- make sure tax and National Insurance contributions are done correctly

Gender reassignment

The moment a worker tells their employer that they're having gender reassignment, they're protected from discrimination. Discrimination includes:

- disadvantaging the worker because of the time they have to take off because of medical treatment
- not enabling the worker to use facilities appropriate to their gender

To avoid discrimination, you must:

- change your records (eg human resources records) when the worker has a Gender Reassignment Certificate and a new birth certificate
- ensure complete confidentiality of all information the worker gives you about their gender history

An employer should be seen to be doing all they can to lessen any risk of unconscious bias affecting management decisions and employees' or interviewees' progression by:

- Considering the wording of job advertisements carefully.

- Ensuring the management team is aware of the biases or actions that may leave the company open to a discrimination claim by providing training on equal opportunities and harassment.

- Ensuring the whole team is aware of what unconscious bias is and the subtle ways it can manifest itself.
  An employer is vicariously liable for the acts of its employees during the course of their employment, with employees being personally liable too.

https://www.equalityhumanrights.com/sites/default/files/ehrc_advertising_-_checklist_12_0.pdf

Bias in machine learning, and how to stop it

AI and machine learning fuel the systems we use to communicate, work, and even travel. But bias seeps into the data in ways we don't always see. Here's why blocking bias is critical, and how to do it.
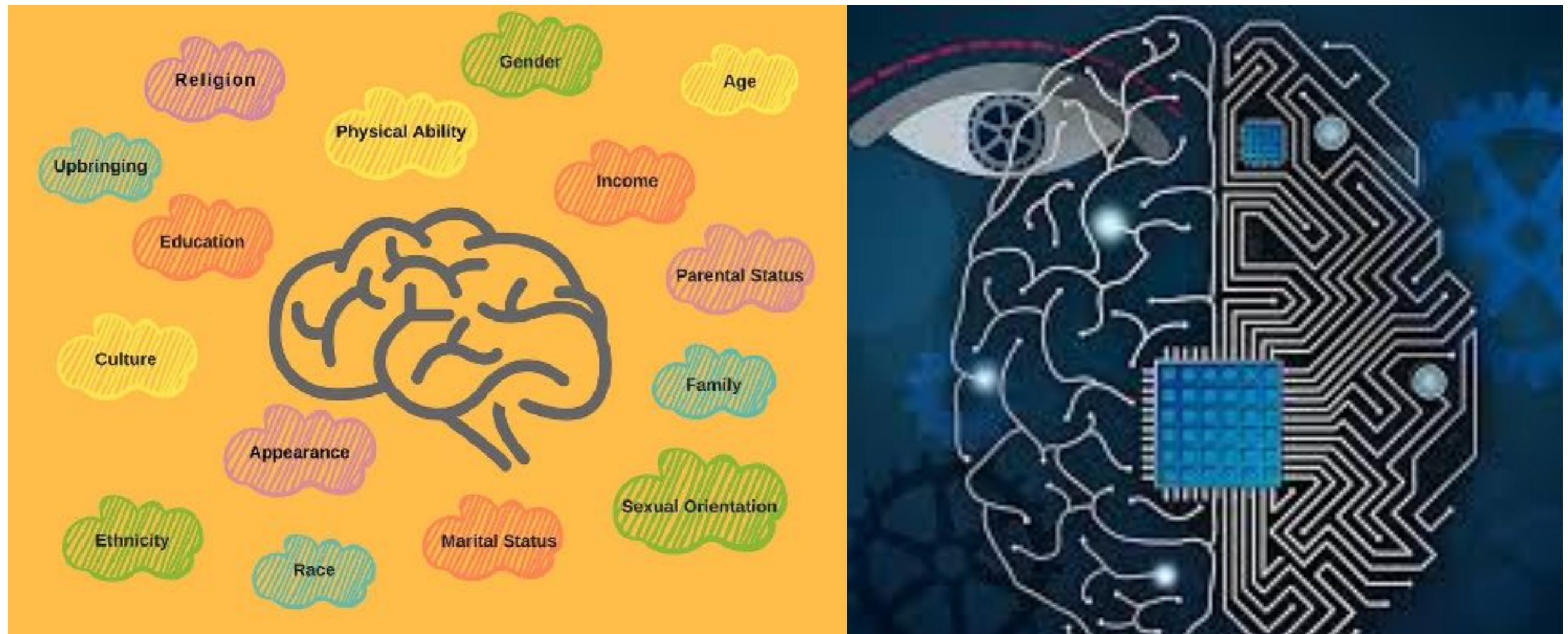
It's critical that organisations ensure that their data and algorithms are checked for bias.

The data we collect – climate, health, energy, and human behavioural data –
should be unbiased, and represent our world fairly.

We have both social and legal responsibilities to ensure that our algorithms are unbiased.
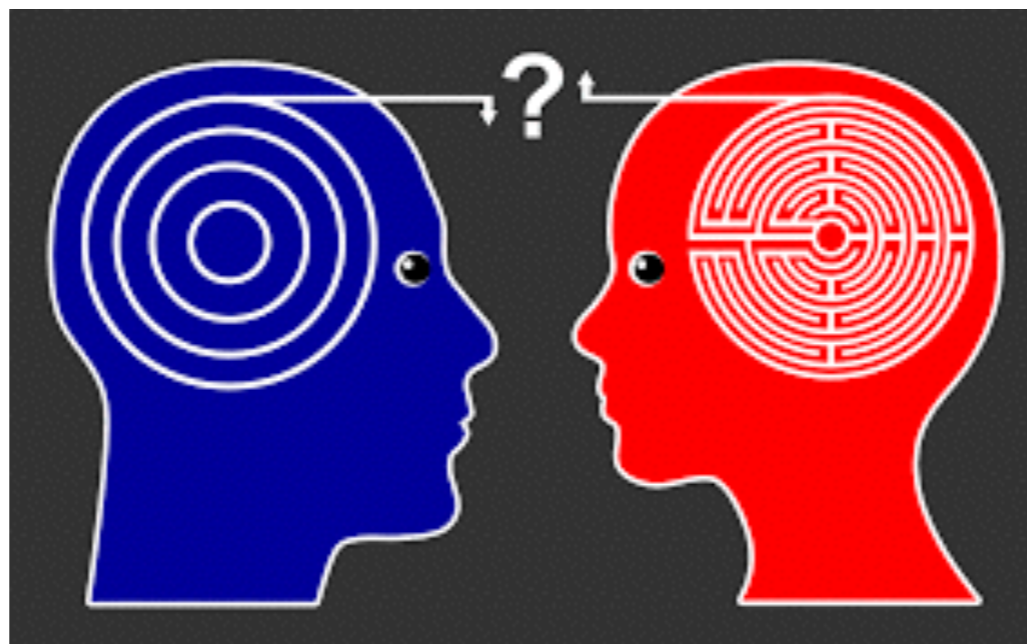
One of the first steps towards unbiasing is education.

Elders

know everything.....
and have all the time in
the world to tell you
about it.
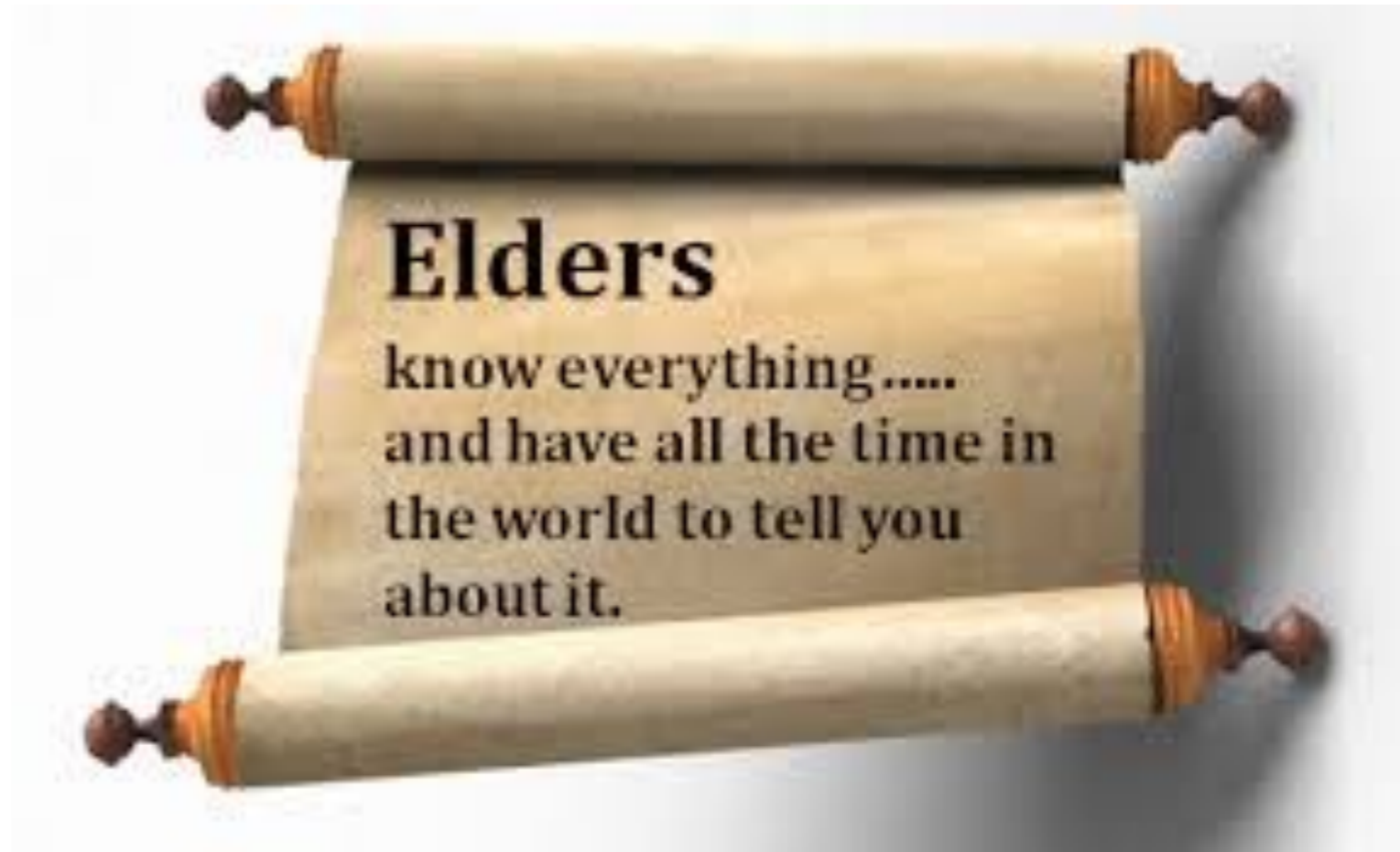
Research shows that
awareness of unconscious bias can lead to reversals in biased outcomes,
and understanding of the unconscious biases that underlie our beliefs may be necessary for changing attitudes.

Ethics Considerations for Information Professionals

Adapted from
Microsoft Information Ethics,
and Columbia University Library
Slides

What is ethics?

- "Ethics is a guide for our morality when we face complicated situations that eclipse the level of our prior moral experience." (Richard W. Severson (1997). <u>The Principles of Information Ethics.</u> Armonk, NY: M.E. Sharpe.

- "Ethics is mostly about how people should be treated and how one should act, if one wishes to act rightly." (Rubin, p. 266)

What is ethics?

- **Ethics is the field of study that is concerned with questions of value**
- **Ethical judgments are concerned with distinguishing "good" or "bad" behavior in a given situation**
- **Ethics include the standards, values, morals, principles, etc., that we use as the basis for our decisions or actions**
- **In ethical decision making, there is often no clear "right" or "wrong" answer**

What is ethics?

- **Ethics refers to well based standards of right and wrong that prescribe what we ought to do**
- **This is usually expressed in terms of rights, obligations, benefits to society, fairness, or specific virtues**
- **It refers to those standards that impose reasonable obligations to refrain from rape, stealing, murder, fraud**
- **It includes those relating to rights (to life, to freedom from injury, to privacy)**
- **These are adequate ethical standards because they are supported by consistent and well founded reasons**

What is ethics?

- **Ethics also refers to the study and development of one's ethical standards**

- **Feelings, laws, and social norms can deviate from what is ethical**

- **It is necessary to constantly examine one's standards to ensure that they are reasonable and well-founded**

- **Ethics means a continuous effort of studying our own moral beliefs and our moral conduct**

- **Through the application of ethics, we strive to ensure that we, and the institutions we help to shape, live up to standards that are reasonable and solidly-based**
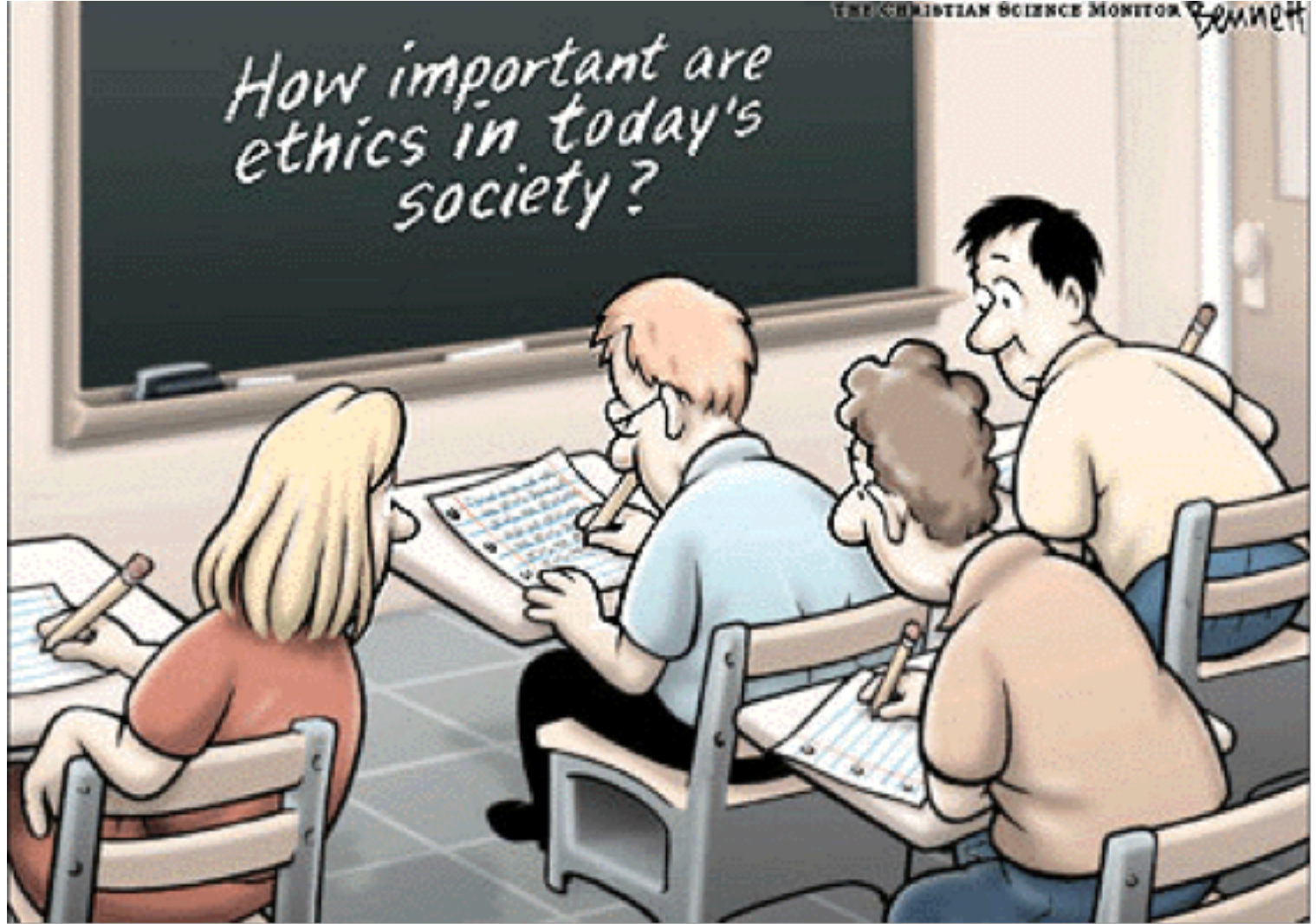
Importance of Ethics

- Ethics provide a framework for
  - Conducting essential information functions
  - Instituting information policies
  - Developing strategies for information services
- Ethical conduct of information professionals is
  - Affirmation of the critical value of services
  - Affirmation of responsibility to themselves and society
  - Affirmation of respect for others
  - Affirmation of the need to improve society

Half a century of issues: from Wiener to IE

The evolution of the <u>information</u> (or rather) <u>data-based society</u> causes <u>ethical problems</u>.

Norbert Wiener (father of cybernetics), in the late 1940s and early 1950s, was the first to predict and work on such problems.

"<u>Computer ethics</u>" coined by Walter Maner in the mid 1970s, to refer to the field of research that studies ethical problems "aggravated, transformed or created by computer technology".

Later, it became clear that what matters is not the specific technology (computers, mobiles, ICTs in general) but the raw material manipulated by it, <u>data/information</u>. So in the late 1990s several researchers, especially our group in Oxford, started working on "<u>information ethics</u>" (IE).

What sort of ethical problems?

1940s/50s (mainframes): (speculative) Robots and humans (Bentham's Panopticon and Orwell's Big Brother, are not digital/computational).

1970s/80s (PCs): PAPA (privacy, accuracy, intellectual property and access), viruses (vandalism).

1990s (Internet): "the triple A": availability, accessibility and accuracy; piracy; digital divide; infoglut; safety, reliability and trustworthiness of complex systems; hacking (vandalism); freedom of expression and censorship; pornography, monitoring and surveillance.

2000 (Infosphere): security and secrecy; propaganda; identity theft.

Add: military, health-related, social, political and religious interpretations (and anthropological, and psychological...).

What kind of interpretation? The Policy Vacuum

<u>Policy Vacuum</u>: technological changes have outpaced ethical developments, bringing about unanticipated problems that have caused a "policy vacuum" filled by CE (Moor, 1985), which has initially surfaced from practical concerns arising in the information society.

Rational decisions have to be taken, technical, educational and ethical problems must be solved, legislation needs to be adopted, codes of ethics are to be formulated and enforced.

A combination of empirical evidence and logical arguments seems to provide the most obvious and promising means to achieve such pressing goals.

How innovative should the approach be?

Which approach? (aka the Uniqueness Debate)

The "no resolution" Approach. CE problems represent unsolvable dilemma and CE is itself a pointless exercise, having no conceptual foundation. (Parker 1981).

The Professional Approach. CE is just a professional ethics. Social responsibility of computer professionals. Development of a professional-ethics approach (Gotterbarn 1991, 1992).

The Radical Approach. CE is a Unique Discipline that deals with absolutely unique issues, in need of a completely new approach (Mason 1986, Maner 1996, 1999).

The Conservative Approach. CE is only an Applied Ethics. Classic macroethics (e.g. Consequentialism, Deontologism, Virtue Ethics, Contractualism) might need to be adapted, enriched and extended, but they have all the conceptual resources required to deal with CE questions successfully and satisfactorily. ICT merely transform old ethical problems. (Johnson 1999).

The Innovative Approach. Information Ethics as the Foundation of CE (Floridi 1999, 2004). According to IE, standard macroethics are insufficient. ICT, by transforming in a profound way the context in which moral issues arise, not only adds interesting new dimensions to old problems, but leads us to rethink, methodologically, the very grounds on which our ethical positions are based.

Need for Discussing Ethical Issues

- Systems that collect, store, process, and act on information may have ethical consequences.

An Innovative Approach: Information Ethics

Information Ethics is the theoretical foundation of applied Computer Ethics.

IE is an expansion of <u>environmental ethics</u> towards

1) <u>a less anthropocentric concept of agent</u>, which now includes also non-human (artificial) and non-individual (distributed) entities; and

2) <u>a less biologically biased concept of patient</u> as a 'centre of ethical worth', which now includes not only human life or simply life, but any form of existence.

3) a conception of environment that includes both <u>natural and artificial (synthetic, man-made) eco-systems</u>.

IE is therefore

- non-standard
- patient-oriented, not agent-oriented
- environmental, non-anthropocentric but ontocentric, and based on the concepts of informational object/infosphere/entropy rather than life/ecosystem/pain.

Four Principles of Information Ethics

IE determines what is morally right or wrong, what ought to be done, what the duties, the "oughts" and the "ought nots" of a moral agent are, by means of four basic principles:

0. entropy ought not to be caused in the infosphere (null law)
1. entropy ought to be prevented in the infosphere
2. entropy ought to be removed from the infosphere
3. the welfare of the infosphere ought to be promoted by extending it, improving it and enriching it.

The principles are listed in order of increasing moral value. They clarify, in very broad terms, what it means to live as a responsible and caring agent in the infosphere.

Three Basic Elements in Professional Ethics

- Self: the moral agent who acts or suffers the consequences of others' actions

- Organization: an institution acting in an autonomous manner

- Environment: the standards of the community/professional societies

Ethics in Informatics
Two Foci

- Information ethics: Use and misuse of information
  - Ownership of information
  - Intellectual property rights
  - Free or restricted access to information
  - Use of government information
  - Assurance of privacy and confidentiality
  - Data integrity
  - International flow of information
  - Actions based on information

- Professional ethics: profession conduct/behavior
  - How information professionals apply ethical principles to decisions and actions
  - Are closely related to information ethics and often overlap with it

Four Important Factors in Ethical Deliberations

- Social Utility
- Survival
- Social responsibility
- Respect for the individual

Four Questions for Organisations
Involved in Ethical Deliberations

- To what extent is the survival of the organization threatened?
- To what extent will the purpose of the organization be benefited or harmed?
- To what extent is the organisation or employee socially responsible or irresponsible when acting in a particular manner?
- To what extent are the actions of the organization or individuals acting in its behalf harming or benefiting other individuals, organisations, or the profession?

Categories of Ethical Concern

- Free access to information/effects of information
- Selection decisions
- Privacy
- Copyright
- Information organization
- Information policy
- Information quality
- Physical consequences

Categories of Ethical Concern

- ## Administrative issues
  - Ethical issues of consultants
  - Ethical obligations to those doing business with the organisation
  - Ethical aspects regarding the treatment of personnel
  - Violation of privacy
  - Misuse of authority
  - Organizational inadequacies

Professional Considerations in Ethical Deliberations
http://www.bcs.org/category/6030

BCS Code of Conduct

sets out the professional standards required by BCS as a condition of membership

applies to all members, irrespective of their membership grade,
    the role they fulfil, or the jurisdiction
    where they are employed or discharge their contractual obligations.

governs the conduct of the individual,
    not the nature of the business or ethics of any Relevant Authority

members are expected to exercise their own judgement
    to meet the requirements of the code and seek advice if in doubt

Public interest: you shall

a) have due regard for public health, privacy, security and wellbeing of others and the environment.

b) have due regard for the legitimate rights of Third Parties.

c) conduct your professional activities without discrimination on the grounds of sex, sexual orientation, marital status, nationality, colour, race, ethnic origin, religion, age or or of any other condition or requirement

d) promote equal access to the benefits of IT and seek to promote the inclusion of all sectors in society wherever opportunities arise.

Professional Competence and Integrity you shall:

a) only undertake to do work or provide a service that is within your professional competence.

b) **NOT** claim any level of competence that you do not possess.

c) develop your professional knowledge, skills and competence on a continuing basis, maintaining awareness of technological developments, procedures, and standards that are relevant to your field.

d) ensure that you have the knowledge and understanding of Legislation* and that you comply with such Legislation, in carrying out your professional responsibilities.

Professional Competence and Integrity you shall:

e) respect and value alternative viewpoints and, seek, accept and offer honest criticisms of work.

f) avoid injuring others, their property, reputation, or employment by false or malicious or negligent action or inaction.

g) reject and will not make any offer of bribery or unethical inducement.

Duty to Relevant Authority

Relevant Authority - The term "**Relevant Authority**" is used to identify the person(s) or organisation(s) which has / have **authority** over the activity of individuals in their professional capacity. For practising **BCS** members this is normally an employer or client.

Duty to Relevant Authority
you shall:

a) carry out your professional responsibilities with due care and diligence in accordance with the Relevant Authority's requirements whilst exercising your professional judgement at all times.

b) seek to avoid any situation that may give rise to a conflict of interest between you and your Relevant Authority.

c) accept professional responsibility for your work and for the work of colleagues who are defined in a given context as working under your supervision.

Duty to Relevant Authority

d) **NOT** disclose or authorise to be disclosed, or use for personal gain or to benefit a third party, confidential information except with the permission of your Relevant Authority, or as required by Legislation

e) **NOT** misrepresent or withhold information on the performance of products, systems or services (unless lawfully bound by a duty of confidentiality not to disclose such information), or take advantage of the lack of relevant knowledge or inexperience of others.

Duty to the Profession
you shall:

a) accept your personal duty to uphold the reputation of the profession and not take any action which could bring the profession into disrepute.

b) seek to improve professional standards through participation in their development, use and enforcement.

c) uphold the reputation and good standing of BCS, the Chartered Institute for IT.

Duty to the Profession
you shall:

d) act with integrity and respect in your professional relationships with all members of BCS and with members of other professions with whom you work in a professional capacity.

e) notify BCS if convicted of a criminal offence or upon becoming bankrupt or disqualified as a Company Director and in each case give details of the relevant jurisdiction.

f) encourage and support fellow members in their professional development

Special Ethical Problems with Information Technologies

- Computers are extremely fast
- Computer use is often private and anonymous
- Computer access can be accomplished from great distance
- The electronic medium is easily copied
- Large number of people are easily reached
- A Code of Ethics for Computer Use
  - Ten Commandments of Computer Ethics

Ethics and IT

- **Our increasing reliance on computing and networks has created many benefits for society**
- **However, in addition to intended consequences, every social action also has unintended consequences**
- **The dark side of computing**
  - **Computer crime**
  - **Unreliable hard/software**
  - **Software piracy**
  - **Invasion of privacy**
  - **Hacking and cracking**
  - **Workplace surveillance**
  - **Viruses and worms**
  - **Data mining**

Approaches to Promote Ethical Conduct

- Establishing rules and regulations
- Developing training and education programs
- Punishing individual for ethical violations
- Establishing an ethics code for the organisation
- Hiring and promoting individuals with ethical behaviour and understanding
- Developing a system of rewards for both ethical actions and unethical ones

Discussion

- A patron requests that he be furnished with information that would permit him to build a small bomb, "just big enough to demolish a small, suburban house." Would you, as a reference librarian, provide the information as requested? If not, what would you do, and how would you defend your action?