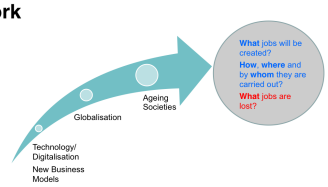
Lecture 1 IT - Productivity and the future of Work

a) Job Market

- high growth in Computer & IT compared to other occupations
  ↳ high avg. pay
- ICT, Software, IT Services strong growth
- Hardware, Consumer Electronics growing less strong
- Internet Industry growing much faster than German Economy

- General decline of wages for young workers
  - In particular, for medium-skilled and low-skilled workers
  - Implies growing wage premia for higher education and rising inequality in wages
- Highly-educated workers have faced declining employment opportunities in top-paying jobs
- Analytical jobs have more positive history overall

Trends Changing Future World of Work



b) Productivity Paradoxon

- hypothesis: increasing productivity due to information technology
- observation: slowdown in productivity growth

↳ depends on measurement of IT intensity (automation vs. computerization)
  > non-manufacturing sectors increased employment
  > manufacturing sectors decreased employment

c) the Future

- Pessimism about the future has always been there
- is there enough new work

new work

greater income, efficiency and flexibility — less social protection and greater precarity] non-standard employment is not new

- growing employment in high income cognitive jobs - problem solving skills
- growing employment in low-income manual service occupations
- loss of employment in middle-income routine jobs

SUM-UP

- IT productivity is generally difficult to measure
- loss of employment in middle-income routine jobs
- new business models may provide new employment opportunities & social tensions
- avoid unemployability unemployable people

Lecture 2 Privacy

a) Data-driven business models

- digital content generated by the users or based on their data
- targeted advertising
- healthcare: precision medicine & extended monitoring — requires health data of many individuals

b) Defining Privacy

- multifaceted concept (surveys gave a variety of meanings)
- Right to be left alone: enjoy life → privacy → be let alone — No invasion into privacy
  ↳ Exceptions: when you are in public, when you published the information yourself
- Boundary Regulation: interpersonal boundaries (shaped physically & by behaviour) create privacy and have to be negotiated
- data as the currency in the digital world → enterprises need to collect data violating privacy.

US-Standard of reasonable privacy expectations

> subjective: persons have tried to ensure their privacy
> objective: would society assess the degree of privacy as reasonable

c) Privacy in Reality

- strong online tracking (even cross device)
- users are concerned about privacy but lacking the knowledge to protect themselves
- Data disclaimers are not read

(Privacy Attitudes)

- Behaviour Shaped by: Lack of information/knowledge, bounded rationality, psychological aspects (i.e. flow state)
- SNS users value their friends privacy lower (third-party-apps request access to friends data, etc.) — Privacy Egoist
  ↳ informing friends about data sharing → less data shared (Context conflicts for SN)

SUM-UP

- data enables new data-driven business models
- data is collected and monetized (data as currency in digital world) agressively
- individuals lack understanding to face privacy issues

Contextual Integrity
- norms of information flow (context mediated)
  ↳ protected by society/law
- decisional privacy

Lecture 3: GDPR

- fundamental right to control data about oneself → established in 2018 following a directive from 1995
  ↳ regulation with some flexibility concretised in national laws

Content

- mandatory Data Protection Offices for controllers (data owner) & processor (acts on behalf of controller)
  ↳ independent accountable advisor and compliance monitorer, cooperation with DPA
- transparent information on data collection and free access to collected data, erasure (right to be forgotten), possible restriction of processing

Controller & Processors responsibilities

> implementation of appropriate security measures considering current technology, cost & possible risk
> notification to DPA on data breach within 72h by controller; processor informs controller immediately
> breach is likely to result in high risk → controller informs affected persons immidiately in plain language
> new measures resulting in high risk → mandatory DPIA (Data Protection Impact Assessment)

- Data must not be transfered to third countries without adequate data protection laws (list provided by EU-C); exceptions possible

Supervisory Authority (e.g. DPA)

> independent monitorer with executive powers

- Privacy by Design
- Some Website blocking EU-users

SUM-UP

- GDPR is a behemoth → will consumers benefit?
- competing regulations exist/ undes development.

Lecture 4: Privacy - Societal Issues

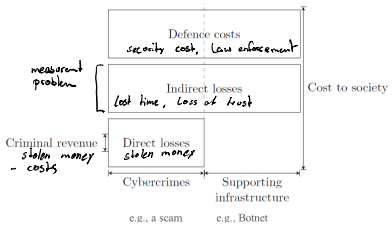
- California Consumer Privacy Act
  ↳ real estate developer gets information on massive privacy issues → submitted ballot with 600.000 signatures with his own lobby-group → intensive lobbying by internet firms → law was passed
- GDPR (faced lobbying, too), high number of complaints in Germany
- Facebook participatory governance system → votes were ignored

Takeaways – Questions

- How do we „manage“ this huge diversity of cybercrimes?
  - How to invest more effectively?
    - Protection
    - Mitigation/Recovery/Self-Insurance
    - Risk-transfer/Cyber-Insurance
    - Do nothing
  - Similar to privacy: Substantial externalities (e.g., bots)
- Can we deal with niche crimes; especially if originating in different jurisdictional settings?

Lecture 5 - Cybercrime

- Defining Cybercrime
  - > traditional forms of crime committed via information systems
  - > publication of illegal content via electronic media
  - > crimes unique to information systems (e.g. DDOS, hacking, etc.)
- Impact of Cybercrime
  - > criminal revenue is really small compared to overall cost for society
  - > high cost for defense (e.g. exchange all payment terminals for new system



- Law Enforcement
  - > difficult due to the need of cross-border cooperation
  - > special technical skills required
  - > police is not informed by those affected
- Types of Cybercrime
  - > fraud, e.g. ad fraud, copyright-infringing, fake companies, fiscal fraud
  - > Sams, e.g. fake antivirus, fake tech support
  - > hacking, e.g. exploiting accounts, ram somware, cyber-espionage

SUM-UP

- huge diversity of cybercrime → how to fight effective on diverse fronts?
- Law enforcemat is difficult due to cross-borders crime and difficult argument ("Beweisführung")
- bad documentation by police as only a fraction of cases is complaint to police
- what is the individuals responsibility - what should be regulated by the states authority

Takeaways

- External and internal drivers push for a systematic information security management
  - Strategic protection of assets, compliance regulations, growing complexity etc.
- Information security management systems (ISMS)
  - Meet security objectives, satisfy external requirements & regulations, improve security-related activities, …
  - Need support for planning, implementation, monitoring, and improvement of an ISMS
- Established standards available to help, but practice is messy
  - ↳ a lot to do

Lecture 6 - Security & Organizations

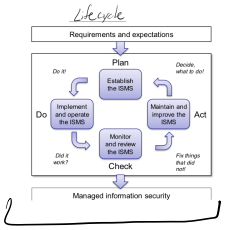
a) Security & Risk management

- concept and scope of security & risk management has evolved with the rise of IT
- more data is needed to provide effective protection (data = key asset)
  - > vertical data-driven collaboration (from sensors etc. to the cloud)
  - > horizontal data-driven collaboration (inter-organization)

b) Information Security Management (- System)

- Why: ensure competitiveness, meet external regulations (e.g. GDPR), efficient security controls, enhance entities structure, required by possible business partners
- ISMS consists of policies, procedures, guidelines, associated ressources
- ISO/IEC 27000
  - > Requirements: Scope, Terms & definitions, leadership, planning, support, evaluation, improvement
  - > Controls: set of control objectives (35) & controls (114) + Documentation
  - > Measurement: difficulty of measuring success unbiased
  - > Risk management: establish -> assess risks -> modify to face risks -> ∞
- How does it work

TODO



SECURITY is a process - not a product!

c) Difficulties

- reliable data missing -> due to lack of complaints
- missing exchange of data between enterprises

SUM-UP

- external & internal drivers push for systematic information security management
- Information Security Management Systems (ISMS)
  - > meet security objectives, satisfy external regulations, improve overall security (activities)
- Standard available (messy!)

Takeaways

- Significant efforts being done towards implementing data collection and processing in the name of national security
- Similar efforts undertaken in many countries regarding Internet filtering and censorship
- Many challenges which are hard to resolve:
  - Grand challenges: Impact on civil liberties
  - More well-defined challenges: Like responsible disclosure

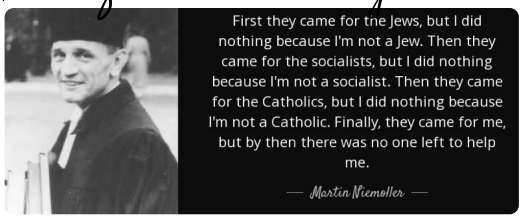
Lecture 7 - Security & Societal Issues

a) Balancing Security & Privacy
- 9/11 lead to patriot act & freedom of information act

b) Programs by Security agencies
- Prism: wiretapping of every "none US-citizen"
- Telecomunications: Providers shifted data to agencies
- Tempora: trans-atlantic fiber taped (21Pb per day) → selectors to sift events
- Muscular: collected unencrypted data flowing between data-centers of large service firms (eg. Google) → they started encrypting internal traffic
- Special Collection Service: collection of electromagnetic emissions (eg. at ambassies)
- Longhaul, Quantum: focus on decryption of encrypted traffic

c) Tools
- Xkeyscore: distributed database enabling easy access for agencies
- Hacking
- Malware provided by private parties
  ↳ control of its deployment?
  ↳ Malware used by black hacks after leaks

d) Nothing-to-hide-argument



→ massive internet filtering
↳ censorship?

SUM-UP

- significant efforts towards data collection & processing for national security
- significant efforts towards internet filtering & censorship
↳ Impact on Civil liberties?

Lecture 8 - Behavioral Insights and Societal Scale Mechanisms

a) From Data to (Behavioral) Insights

- Big Data offers new insights into human emotions/cognitions/motivation/decisions/preferences/behaviors/etc.
- Allows view on behavioral insights → roadmap to change behaviour

b) Nudge Theory

- founded by Richard Thaler (nobel price 2017)

„A nudge, as we will use the term, is any aspect of the choice architecture that alters people's behaviour in a predictable way without forbidding any options or significantly changing their economic incentives."

- people shall make decisions that are in their self-interests
- not about penalising people - about easing decision making (influence choice architecture)
- preserve full freedom of choice - nudged one's do not notice

c) Types of Nudging

- Default option
- Social Proof Heuristics, e.g. „X% of individuals think x", the more local & specific, the more powerful
- Reminder
- Provide Feedback, positive feedback serves as a reinforcer
- Element of Entertainment/Gamification
- Disclosure, operates as a „check"

Critics

- who decides what is the best choice?
  ↳ picture of mankind?
  ↳ subjective
- Nudges are not transparent → manipulative → personal freedom violated

„Feelgood interventions" for Nudging

d) Google's Selfish Ledger

- Collect massive data on people („ledger")
- define goals & get reminders to achieve goals, decisions are made by ledgers rather than by the people themselves

↳ attack on individuals personal freedom?

e) China Social Credit System

- multi-level, nationwide rating system rating residents on honesty and trustworthiness
- Reasons for implementation
  - > moral decline in society → public shaming & praising
  - > strengthening domestic economy → loans based on trustworthiness, lack of information to determine financial trustworthyness
- public blacklist/redlist → highspeed-trains, insurances, private schools, travelling
  - > ensuring the population to behave the way the governments desires

SUM-UP

- behavioral insights used in various fields/countries
  ↳ increasing popularity in digital environments (comp. Google Ledger)
- Nudging: change choice architecture but preserving individuals free choice (default option, social proof heuristics, positive feedback)
- used for surveillance, oppression, etc
  ↳ how to face those threats?

Lecture 9 - Introduction to Artificial Intelligence

a) Definition AI

- No general Definition available
- Different views
  - > thinking humanly (make computers think, machines with minds)
  - > acting humanly (perform function that require intelligence when performed by people)
  - > thinking rationally (computations allowing perceiving → reasoning → acting)
  - > acting rationally (automation of intelligent behavior)
- Make computers do things better than people ("people": no mistakes + access to massive data)
- use power of computers to augment human thinking + understand how humans think

Rational: maximize goal achievement, minimize mistakes

b) Measuring Quality of AI

- Turing Test: computer cannot be distinguished from a human in a conversation
  - > Eliza (Psychotherapist Program) using keywords + pre-canned responses, parroting, highly general questions
  - > Loebner Prize (for a computer passing Turing-Test)
  - > Google Duplex
- Strong AI: matches/exceeds human intelligence
- Weak AI: not intended to match/exceed human intelligence → applied/narrow AI (machines can demonstrate intelligence, but no mind/mental state)
  - ↳ they don't understand, just answer based on rules

c) AI Fears & Hopes

- Fears: Impact on Job Market
- Good: Sustainability, Environment Protection, Health, Transparency, Education)

d) Case Study: Stack Overflow

- Result: bad code tends to be ranked higher (therefore even used in popular Apps)
- Solution: Nudging (Warnings, Recommendations, Reminder, Default (rank secure code higher)
  - ↳ test-groups nudged created better code

SUM-UP

- no general Definition for AI due to different facets, focus on acting rationally (automation of intelligent behavior)
- quality is measured by distinguishability from human
- Fears, Hopes & Expection in Society

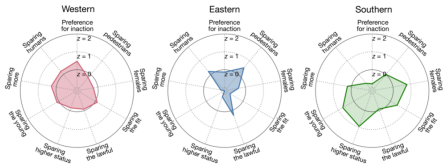
Lecture 10 - Ethics of AI

a) Ethics / Moral philosophy

- Utilitarianism: What creates the most overall utility for the individuals involved? (consequentialist principle)
- Deontology: What is the intrinsic quality of the act itself? (categorical principles)
- Virtue Ethics: emphasizes virtues (dt. Tugenden) or moral character

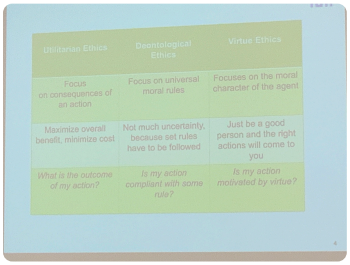
b) Moral Machine

- huge global study researching moral decisions
- strong cultural differences
  ↳ implement in AI (e.g. AV)?



c) Moral for AI

- Ethics Comission on AV only in Germany
- we would be better overall with utilitarian cars
  ↳ but people want cars protecting them



SUM-UP

- Major approaches: deontology, utilitarianism, victue ethics
- digital technologies (especially AI) create morally charged decisions
  ↳ who is supposed to define thes decision (with regards to cultural differences)

Lecture 11 - Fairness, Accountability & Transparency

a) Why FAT matters

- algorithms make/support decision: fair decision (Fairness), who made it (Accountability), how was it made (Transparency)
- Ethics → trust-enhancing factors (FAT) → product adoption

b) Case Study: Compass

- Compass risk predicting software by private company → algorithm is proprietary → trade secret → little transparency
- analysis on 7.000 people 2013-2014 (Florida)
  - ↳ only 20% of people predicted to commit violent crimes actually committed
  - ↳ only 50% of people predicted to commit misdemeanors actually committed
  - ↳ overall 61% → high percentage of Type I-Error
  - ↳ fair? algorithms can just implement one conceptualization of fairness
- Northpoints Fairness definitions: risk scores map to equal probability in actual re-offending (same true positive) [but the number of blacks scored medium/high risk is bigger]
- ProPublicas Fairness definition: risk distribution across „high" and „low" differs across race, therefore ratio (different positive rates) [but dataset is biased - not the algorithm]
- Antidiscrimination Law VS: Race, Color, Sex, Religion, Origin, Citizenship, Age, Pregnancy, Family status, Disability status, Veteran status, Genetic information

calculated \ actually true	H_0	H_A
H_0	True negative	False negative
H_A	False positive	True positive

c) Bias in Data

- Algorithm learned from biased data → algorithm biased
- broken window theory: neighbourhood with visible civil disorder → more police forces → more arrests ?
  - ↳ certain attributes occur more often in dark zones

d) Transparency

- GDPR provides „a right to explanation" → meaningful information on logic involved, significance, envisaged consequences
  - ↳ Explanation: create transparency → create accountability → create trust
- ex ante: explanation before decision was made
- ex post: explanation after decision was made

SUM-UP

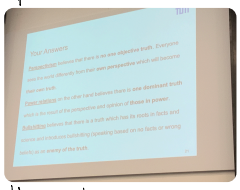
- Fairness, Accountability & Transparency can serve as ethical measurements & trust enhancing factor → product adoption
- biased data: algorithms may outperform humans in some tasks, but the consistently discriminate if data is biased
  - ↳ raw data is oxymoron ← problem for all ML-based systems
- algorithms can only implement one conceptualization of fairness
  1. Treating similar individuals similarly.
  2. Never favor a worse individual over a better one.
  3. Calibrated fairness.
- GDPR contains right to explanation - but only ex ante

Lecture 12 - Misleading Information and Fake Advice

a) Deceptive & Misleading Marketing Practices - Dark Pattern

- 1,818 instances of Dark Pattern on 11000 most popular retail sites
- Sneaks into Baskets: adding additional products to basket (without consent)
- Hidden Cost: added just before checkout (sunk cost fallacy cognitive bias)
- Hidden Subscription: charging recurring fee under pretense of one-time free trial
- Deceptive Countdown Timers: showing time until offer „expires" (often fake)
- Limited-time Messages: without deadline, thereby creating uncertainty and urgency
- Confirmshaming: decisions are linked to emotions
- Visual inference: style and visual presentation to influence users (e.g. greying option, although they are possible)
- Trick Question/Phrases: e.g. beginning with affirmative statement, use of double negatives
- Pressured Selling: use of defaults & high-pressure tactics for up- and crossselling
- Social Proof: determination of the correct action by examing behaviour of others; exploit
- Low-Stock Messages: triggers uncertainty
- Obstruction: make certain actions harder than others, e.g. canceling subscription
- Forced Action: Combine required takes with additional ones

→ offered by certain third party entities



b) Solving the issue

- Technolog Solution: Browser plugin warning users on dark patterns
- Legal Solution: DETOUR Act prohibiting usage of dark patters & behavioral experiment with customers

c) Fake Advice, Post-truth & Alternative Facts

- objective facts are less influential in shaping public opinion than appeals to emotion & personal beliefs
- Nietzsche: objectiv truth is a relic - there are perspectives; we agree on things not because they're true but by virtue of sharing same perspective
- Foucault: no absolute truth, just different regimes of truth - ongoing discourse: what is current truth ← „Power Relation"
- Frankfurt: bullshitting is greater enemy of truth than lies are
  ↳ bullshitting happens whenever someone is required to talk about something he has no idea of

- Dual Processing Model: System 1 (95%): fast, automatic, impulsive, associative, emotional; System 2: slower, conscious, reflective, analytical, rational
  ↳ Gilbert: load and time pressure increase usage of System 1 making humans susceptible for lies
- Exploit: Propagation of Confusion, Businesses based on alternative facts

SUM-UP

- usage of dark patters to increase conversion rates by tricking users
  ↳ solution: technical (browser plugin) & Lawmaking (DETOUR) prohibiting such dark patterns
- no objective truth
- Two stage information processing

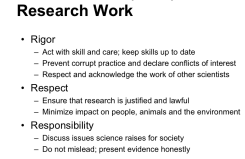
Lecture 13 - Research and Ethics

a) Definitions
- responsibility of researchers to be honest and respectful to those affected by the research study
- set of moral & social standards including prohibitions against and prescription for specific behaviour in research

b) Nuremberg Code
- doctors trial in Nuremberg (NS) → defense: no law defining legal & illegal medical research → 10 standards Nuremberg Code was created
  ↳ influenced by Hippocratic Oath
  ↳ voluntary consent of subject; fruitful result for society, which can not be aquired in different ways; based on animal experimentation; avoid all unnecessary physical & mental suffering/injury; should not be conducted with prior reason to believe death/serious injury could occur; balance of risk&benefits; preparations to protect subjects against injury/disability/death, conducted by scientifically qualified persons; human subject can end experiment at any time; transparency on potential harms (at any time)

c) Discussed Research
- Tuskegees Syphilis Study: participants didn't get ending treatment (penicillin) to treat their disease → instead placebo → many died + infected more people
- Milgram Experiment: „giving" electric shocks to another humans instructed by authority → really difficult to stop → some participants traumatized

d) Currently
- Universities have Institutional Review Board
- Belmont Report incl. basic ethical principles: respect for persons (people incapable of making their own choices should be protected, consent to participate), benefice (balance potential benefits and harms), justice (fair distribution of costs & benefits to pot. research participants)
- Deception must be justified
  ↳ passive: researchers do not tell participants about studies purpose
  ↳ active: researchers mislead subjects about studies purpose
- difficulties in balancing ethics & methodology



e) Industrial Research
- Facebook did behavioural experiments on their user (accepted by their Data Use Policy)
  ↳ result were published although it does not follow rules of institutional research

SUM-UP

- research should be conducted to study and make progress on pressing issues
  ↳ conducted ethically (respect for persons, benefice, justice; Nuremberg Code)
  ↳ history of problematic studies
- digital platforms involved in research
  ↳ poor notice & consent, no actual choice
- difficulties in balancing ethics & methodology