Computer Misuse Act (CMA)

Rogério de Lemos

Based on E. Boiten, B. Keim, K. Welsh slides

University of Kent

CMA

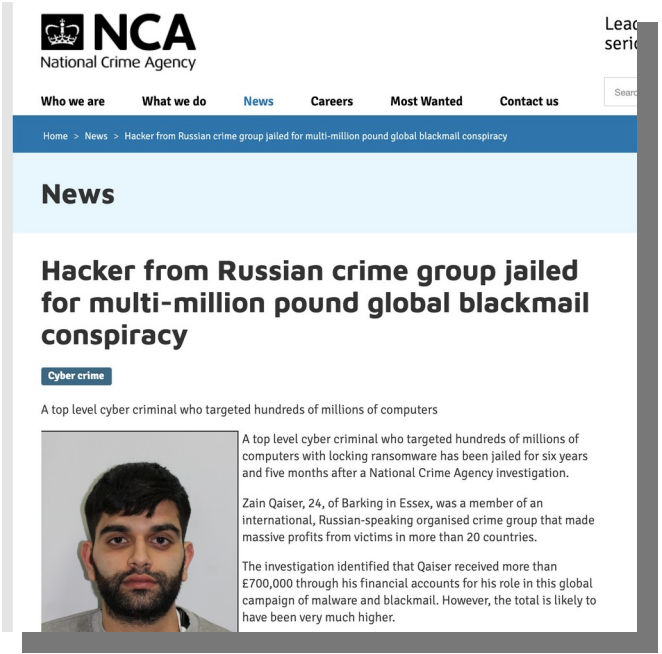
LETS START WITH SOME CASES

Computer Misuse Act 1990 cases

http://www.computerevidence.co.uk/Cases/CMA.htm

R v Zain Qaiser

- Kingston Crown Court 8 April 2019
- Computer Misuse Act 1990 s3 Unauthorised acts with intent to impair; Blackmail; Fraud by false representation; Possessing criminal property



Computer Misuse Act 1990 cases

http://www.computerevidence.co.uk/Cases/CMA.htm

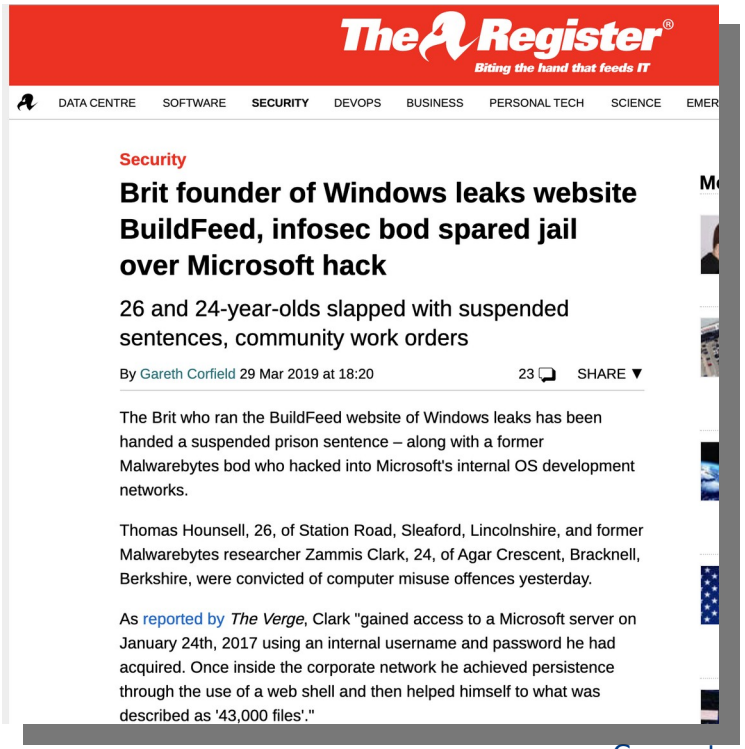
- Multi-million pound global blackmail conspiracy
- Between 2012 and 2014 Computer Science student Qaiser, 24, planted ransomware attacks (using Angler Exploit Kit) on porn websites designed to display threatening warning messages from the FBI or local police force and to lock users' computers (using Reveton or Cryptolocker)
- National Crime Agency investigation. Defendant initially claimed that he had been hacked
- Guilty plea to four CMA charges. Sentenced to six years and five months prison
- Widely reported as the UK’s most serious cybercrime case

Computer Misuse Act 1990 cases

http://www.computerevidence.co.uk/Cases/CMA.htm

R v Zammis Clark and Thomas Hounsell

- Blackfriars Crown Court 28 March 2019
- Computer Misuse Act 1990 s3 Unauthorised acts with intent to impair



The Register®
Biting the hand that feeds IT

DATA CENTRE SOFTWARE SECURITY DEVOPS BUSINESS PERSONAL TECH SCIENCE EMER

Security

Brit founder of Windows leaks website BuildFeed, infosec bod spared jail over Microsoft hack

26 and 24-year-olds slapped with suspended sentences, community work orders

By Gareth Corfield 29 Mar 2019 at 18:20 23 SHARE ▼

The Brit who ran the BuildFeed website of Windows leaks has been handed a suspended prison sentence – along with a former Malwarebytes bod who hacked into Microsoft's internal OS development networks.

Thomas Hounsell, 26, of Station Road, Sleaford, Lincolnshire, and former Malwarebytes researcher Zammis Clark, 24, of Agar Crescent, Bracknell, Berkshire, were convicted of computer misuse offences yesterday.

As reported by *The Verge*, Clark "gained access to a Microsoft server on January 24th, 2017 using an internal username and password he had acquired. Once inside the corporate network he achieved persistence through the use of a web shell and then helped himself to what was described as '43,000 files'."

Computer Misuse Act 1990 cases

http://www.computerevidence.co.uk/Cases/CMA.htm

- Security researcher Clark, 24, aka Slipstream / Raylee and Hounsell, 26, hacked into Microsoft OS software development systems, downloaded 43,000 files and shared details of their exploits online with other hackers; damage estimated at $2M
- Clark also hacked into Nintendo systems and stole 2,000 user ID credentials; damage estimated at £1.4M
- Autistic Clark pleaded guilty to three CMA charges. Sentenced to 15 month prison sentence suspended for 18 months, rehabilitation activity order (25 days), 5 year serious crime prevention order and £140 victim surcharge
- Hounsell pleaded guilty to one CMA charge. Sentenced to 6 month prison sentence suspended for 18 months, unpaid work order (100 hours) and £115 victim surcharge

Computer Misuse Act 1990 cases

http://www.computerevidence.co.uk/Cases/CMA.htm

R v Steffan Needham

- Reading Crown Court 1 March 2019
- Computer Misuse Act 1990 s1 Unauthorised access, s3 Unauthorised acts with intent to impair

The Register®
Biting the hand that feeds IT

DATA CENTRE SOFTWARE SECURITY DEVOPS BUSINESS PERSONAL TECH SCIENCE

Data Centre ▸ Cloud

Vengeful sacked IT bod destroyed ex-employer's AWS cloud accounts. Now he'll spent rest of 2019 in the clink

Bloke hit delete on £500,000 of 'business-critical data' after he was let go for 'poor' performance

By Gareth Corfield 20 Mar 2019 at 15:44 103 SHARE ▼

Computer Misuse Act 1990 cases

http://www.computerevidence.co.uk/Cases/CMA.htm

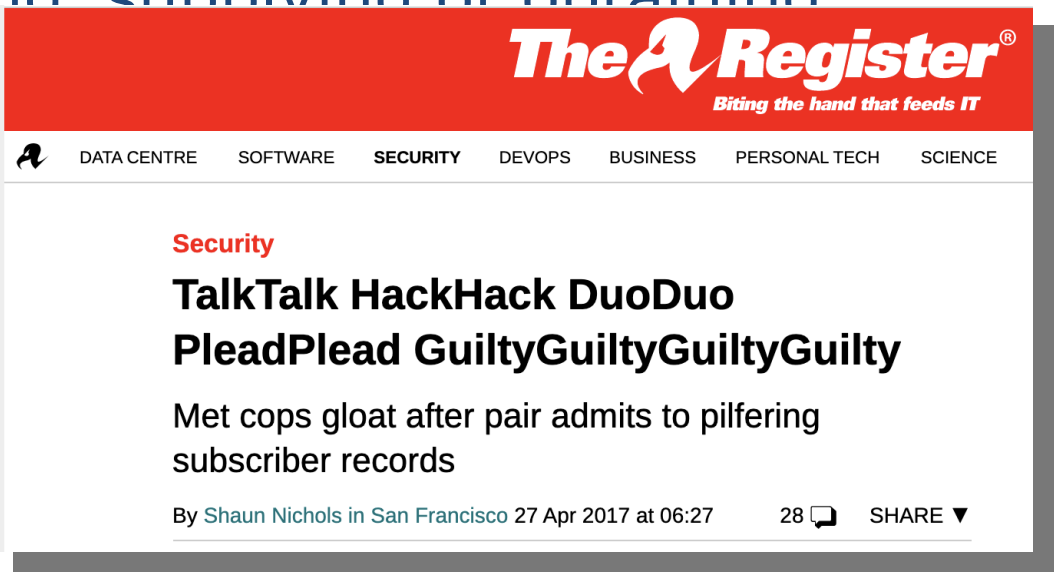
- Sacked IT consultant Needham, 36, used a former IT colleague's Login ID to delete client data on his former employer Voova's 23 servers. Losses estimated at £500,000 and several redundancies resulted
- Found guilty. Sentenced to two years in prison

Computer Misuse Act 1990 cases

http://www.computerevidence.co.uk/Cases/CMA.htm

R v Matthew Hanley and Connor Allsopp

- Central Criminal Court 19 November 2018 Court of Appeal (Criminal Division) 30 January 2019
- Computer Misuse Act 1990 s1(1) Unauthorised access, s3A Making, supplying or obtaining articles; Fraud



Computer Misuse Act 1990 cases

http://www.computerevidence.co.uk/Cases/CMA.htm

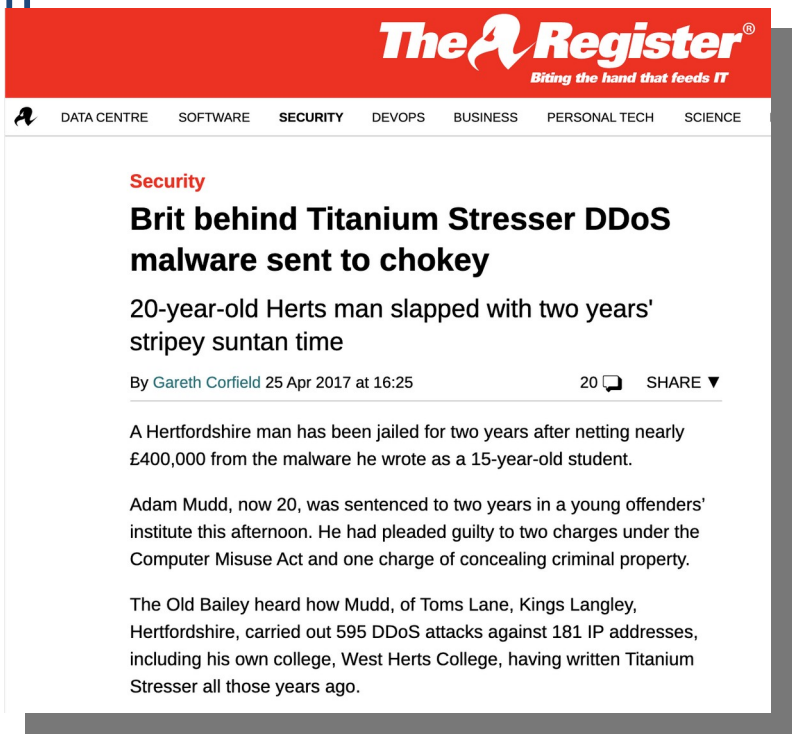
- Hanley, 23, and Allsopp, 21, stole more than 150,000 customer records in the £77 million 2015 attack on TalkTalk website vulnerabilities to DDoS and SQL injection attacks.
- Guilty pleas. Hanley sentenced to 12 months jail and Allsopp to eight months
- Allsopp's appeal against sentence failed.

Computer Misuse Act 1990 cases

http://www.computerevidence.co.uk/Cases/CMA.htm

R v Adam Mudd

- Central Criminal Court 25/04/2017, 27/03/2018
- Computer Misuse Act 1990 s3 Unauthorised acts with intent to impair



The Register®
Biting the hand that feeds IT

DATA CENTRE SOFTWARE SECURITY DEVOPS BUSINESS PERSONAL TECH SCIENCE

Security

Brit behind Titanium Stresser DDoS malware sent to chokey

20-year-old Herts man slapped with two years' stripey suntan time

By Gareth Corfield 25 Apr 2017 at 16:25 20 SHARE ▼

A Hertfordshire man has been jailed for two years after netting nearly £400,000 from the malware he wrote as a 15-year-old student.

Adam Mudd, now 20, was sentenced to two years in a young offenders' institute this afternoon. He had pleaded guilty to two charges under the Computer Misuse Act and one charge of concealing criminal property.

The Old Bailey heard how Mudd, of Toms Lane, Kings Langley, Hertfordshire, carried out 595 DDoS attacks against 181 IP addresses, including his own college, West Herts College, having written Titanium Stresser all those years ago.

Computer Misuse Act 1990 cases

http://www.computerevidence.co.uk/Cases/CMA.htm

- Teenager Mudd wrote Titanium Stresser DDoS malware and used it for 595 DDoS attacks against 181 IP addresses. Received Rental Income of some £386,000 from 112,000 registered users
- Guilty plea. Sentenced to two years in a young offenders institute. Ordered (27 March 2018) to pay back £70k within three months or face further two years detention

University of Kent

CMA

WHEN ALL STARTED

R v Gold & Schifreen

- Robert Schifreen and Stephen Gold, using conventional home computers and modems in late 1984 and early 1985, gained unauthorized access to British Telecom's Prestel interactive *viewdata* service
- While at a trade show, Schifreen, by doing what later became known as shoulder surfing, had observed the password of a Prestel engineer: the username was ‘22222222’ and the password was ‘1234’
- Armed with this information, the pair explored the system, even gaining access to the personal message box of Prince Philip, Duke of Edinburgh

University of Kent

R v Gold & Schifreen

- Unknown to Schifreen and Gold, the Prestel computer network operated on a distributed basis and was intended to act as a hot standby in the event of the UK going to war — in the event that the primary UK military computers were down, the Prestel network could be used to control and launch the UK's nuclear missiles
- Initially convicted (under the Forgery and Counterfeiting Act 1981), they received small fines

R v Gold & Schifreen

- After the initial ruling, the case went to the court of Appeal and then to the House of Lords
- The specific House of Lords decision1988 was interpreted to mean that hacking was not a criminal offence

University of Kent

R v Gold & Schifreen: From the ruling of the Lords

"We have accordingly come to the conclusion that the language of the Act was not intended to apply to the situation which was shown to exist in this case. The submissions at the close of the prosecution case should have succeeded. It is a conclusion which we reach without regret. The Procrustean attempt to force these facts into the language of an Act not designed to fit them produced grave difficulties for both judge and jury which we would not wish to see repeated. The appellants' conduct amounted in essence, as already stated, to dishonestly gaining access to the relevant Prestel data bank by a trick. That is not a criminal offence. If it is thought desirable to make it so, that is a matter for the legislature rather than the courts."

Lord Brandon of Oakbrook

University of Kent

Results (1988)

- Possible Interpretation: No hacking offense (Or at least no offense under the Forgery and Counterfeiting Act)
- Security aspects of the system may be relevant
  The user name was 22222222
  The password was 1234
- Technical aspects of computing, especially telecomputing can have complex effects that previous laws don't take into account
- High publicity
- Mixed aspects of hacking (It may be done for a number of purposes: good fun, serious disruption, malice)

University of Kent

CMA

COMPUTER MISUSE ACT

1990 Computer Misuse Act - brief summary

The Act started with three new criminal offences and has 4 **since 2006**:

1. Unauthorised access to computer material
2. Unauthorised access to computer material with intent to commit or facilitate commission of further offences.
3. Unauthorised **acts with intent to impair operation of computer** etc

3A. Making, supplying or obtaining articles for … (1,3)

1990 Computer Misuse Act - brief summary

1. Unauthorised access to computer material

- Described by the Act's sponsor as 'simple hacking' - using a computer without permission
  - This carries a penalty of up to two years in prison or a fine
- Involves causing a computer to perform some function.
  - But could be as little as **guessing and using a password**

1990 Computer Misuse Act - brief summary

2. Unauthorised access to computer material with intent to commit or facilitate commission of further offences.
   - Covers actions such as attempting to use the contents of an email message for blackmail.
     - This is a more serious offence, and the penalty is up to five years imprisonment and an unlimited fine.

1990 Computer Misuse Act - brief summary

3. Unauthorised modification of computer material.
   - Covers distributing a computer virus, or malicious deletion of files, & direct actions
     - e.g. altering an account to obtain fraudulent credit
   - From 2006 Police & Justice Act, rephrased as: Unauthorised **acts with intent to impair operation of computer …**
     - as it was up to then unclear whether denial-of-service was CMA.
   - The Act also includes the offences of conspiracy to commit and incitement to commit the three main offences.

1990 Computer Misuse Act - brief summary

- Maximum penalty for §3. raised to 10 years and unlimited fine in 2006.

3A. Making, supplying or obtaining articles for … (1,3)

- Computer viruses, worms, Trojans, malware, malicious scripts etc
- which carries max. 2 years and a fine.

- 2015 Serious Crime Bill: made hacking by intelligence services legal. ("clarified" – hacking has since gone into IP Act) + 3A procurement of tools

1990 Computer Misuse Act - brief summary

- Finally, the Act attempts to cover international computer crime
- The act is an example of a law using the “objective territoriality principle”
  - crime committed here if any of the elements (e.g. the effects) are here
- Hacking into a computer in Milan from a terminal in London is illegal (as is hacking into London from Milan). (Routers!?)

DPP v Bignell [1998]

- Two police officers, who were authorised to request information from the police national computer (PNC) for policing purposes only, requested a police computer operator to obtain information from the PNC which, unbeknown to the operator, was for their own personal use.
- Acquitted after appealing
  - "Extracting data from computer by a person who was otherwise generally authorised to use the computer"

Computer Misuse Act 1990
1. Unauthorised access to computer material.
(1) A person is guilty of an offence if—
(**b**) the access he intends to secure is unauthorised; **and**
(**c**) He knows at the time when he causes the computer to perform the function that that is the case.

R v Bow Street Magistrates' Court and Allison

- A Florida-based American Express employee had authorisation to access customer information, but she got information from other accounts and passed it on, which allowed fake credit cards to be produced. The defendant was arrested in London in possession of some of these credit cards. Extradition procedures were initiated. Allison's attorneys alleged that none of the offences were worthy of extradition.

S17(interpretation).5. Access of any kind by any person to any program or data held in a computer is unauthorised if -
(a) he is not himself entitled to control access of the kind in question to the program or data; and
(b) he does not have consent to access by him of the kind in question to the program or data from any person who is so entitled.

R v Bow Street Magistrates' Court and Allison

- Subsection 5 of the CMA (s.17 – interpretation) alongside the prior DPP v Bignell case lead Bow Street to rule in favour of Allison
- When appealed by the prosecution, the House of Lords rejected the s.17 argument and overturned the decision (citing subsection 2)
  - This, in turn, overturned the DPP v Bignell case

2. A person secures access to any program or data held in a computer if by causing a computer to perform any function he--

(a) alters or erases the program or data;
(b) copies or moves it to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held;
(c) uses it; or
(d) has it output from the computer in which it is held (whether by having it displayed or in any other manner);

and references to access to a program or data (and to an intent to secure such access) shall be read accordingly. .....

5. Access of any kind by any person to any program or data held in a computer is unauthorised if -

(a) he is not himself entitled to control access of the kind in question to the program or data; and
(b) he does not have consent to access by him of the kind in question to the program or data from any person who is so entitled.

R v Bow Street Magistrates' Court and Allison

- Subsection 5 of the CMA (s.17 – interpretation) alongside the prior DPP v Bignell case lead Bow Street to rule in favour of Allison
- When appealed by the prosecution, the House of Lords rejected the s.17 argument and overturned the decision (citing subsection 2)
  - This, in turn, overturned the DPP v Bignell case

"Read as a whole, the Report makes it clear that the term "hacking" is used conveniently to refer to all forms of unauthorised access whether by insiders or outsiders and that the problem of misuse by insiders is as serious as that by outsiders. The offence should cover a person who causes the computer to perform a function when he "should know that *that* access is unauthorised". An employee should only be guilty of an offence if his employer has clearly defined the limits of the employee's authority to access a program or data."

Gary McKinnon and Lauri Love

- Both (2001/2; 2013-) accused of hacking US computers
- Both autistic
- Objective extraterritoriality: you'd think they'd get prosecuted in UK, but no …
- US extradition on the cards for both: McKinnon from 2005-2012 when finally dropped for humanitarian reasons; Love decided 2016 still appealing.
- Why not under CMA? McKinnon: evidence in US; Love: not charged in UK despite NCA arrest.

Issues – what's a computer

The Computer Misuse of Act doesn't define what a computer is.

- (What about cars, cameras, … that incorporate computers? Most have argued that a narrow view of what is a computer should be followed.)
- A number of other countries have apparently followed this principle (France and Germany)
- Smart phones may need to be added (Phone Hacking scandal 2011)

The US Computer Fraud and Abuse Act does define computers

- 'an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.' [cited in Reed and Angel, 303]

Another definition, Council of Europe Convention on Cybercrime

- any device or a group of inter-connected or related devices, one or more of which, pursuant to a program, performs automatic processing of data [cited in Reed and Angel, 303]

2015 updates to the CMA

- Updated in May in relation to the Serious Crime Act 2015
- Section 3ZA: If classed as ‘serious’, may face life imprisonment
  - Section 3ZA- Unauthorised acts causing, or creating risk of, serious damage.
  - Section 3ZA is primarily aimed at those who seek to attack the critical national infrastructure
    - Depending on the motives of the perpetrator, terrorist legislation may be appropriate
- Section 10 ‘Savings’: GCHQ, intelligence officers and police exempt from prosecution

University of Kent

CMA

THE LEGAL SIDE

University of Kent

Basics

- Law
  - ignorance never an excuse
  - common sense may not apply!
- Disclaimer
  - this is not a lecture explaining law but one pointing out law that may be relevant
- Insights to computer/software related law
  - Data Protection, Computer Misuse, Professional Issues, IPR, Equality

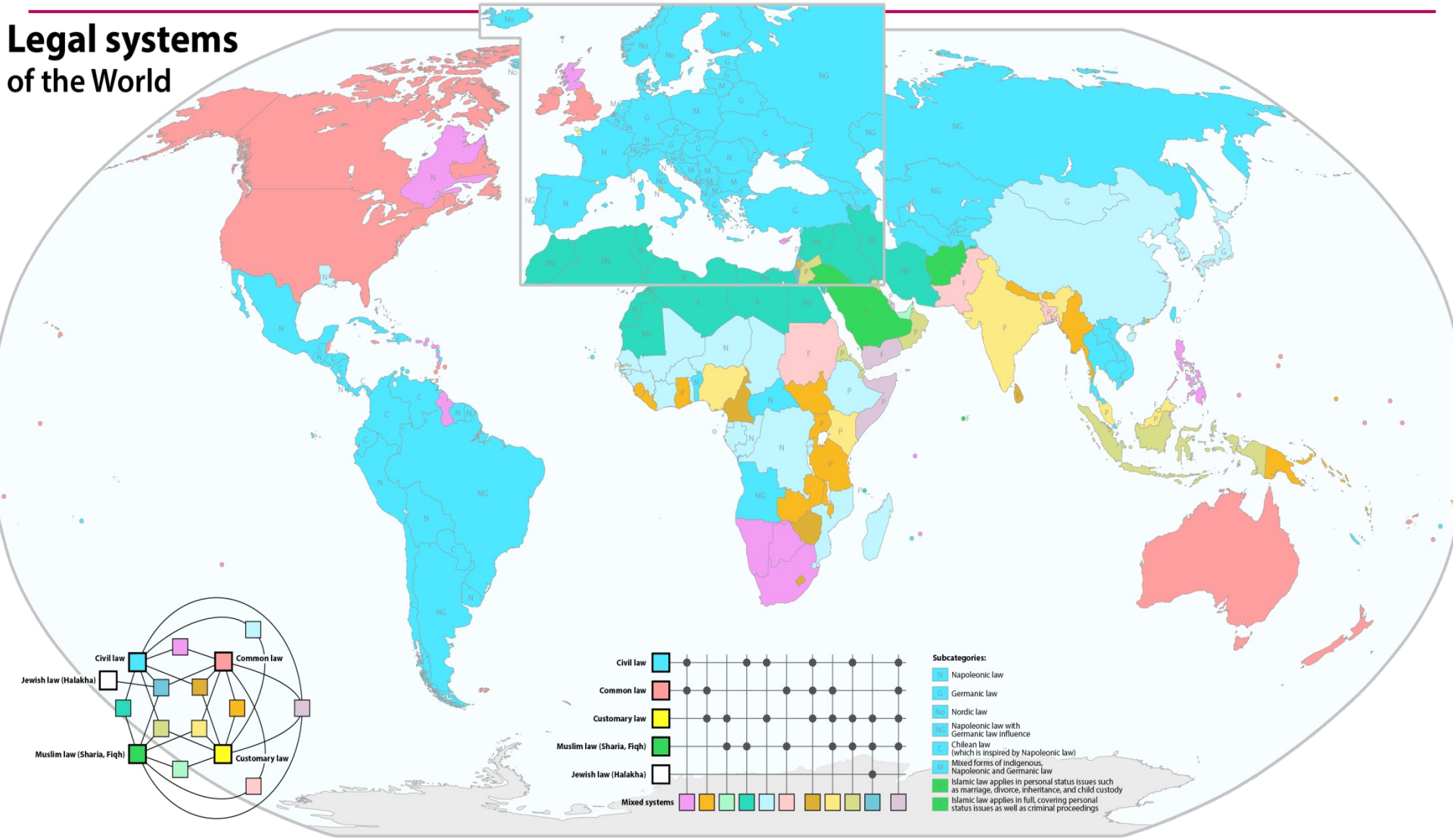
Systems, courts & lawyers

Two different basic legal systems in use around the world

- Common Law - emphasises precedent
  - A legal precedent made by a judge during the course of a case / fluid and interpretive / a judge applies knowledge of legal precedent (prior decisions) and common sense to the facts / cases are individual (unique) / English law works on a common law system / adversarial system / single decided case becomes binding law
- Civil Law - emphasises codified rules
  - A referable system of codified principles / based on more generalised concepts, categories and rules / basis in natural law, codification and legal positivism / places statutory law over case law / secures the rights and duties of individuals / inquisitorial system / long series of cases connected with consistent reasoning required to change law
- Religious Law (either Canon law or sharia)

University of Kent

Systems, courts & lawyers



Brief overview of UK Law

UK: Complex structure

- English law (for England and Wales)
- Northern Ireland Law
- Scottish Law

Sources of English law

- Acts of Parliament
- Secondary Legislation
- Precedent – ('case law', 'common law' – previous decisions)
- EU Law (Regulations, Directives and Decisions)

Brief overview of UK Law

- Criminal Law
  - Prosecution of a person for an act classified as a crime / prosecution by the state (R) / potential for incarceration / no act is a crime unless previously established as such by statute or common law / secures boundaries of acceptable conduct / high burden of proof
- Civil Law
  - Non-criminal law / no potential for incarceration / typically seeking compensation for injury over infliction of punishment / low burden of proof

Brief overview of UK Law

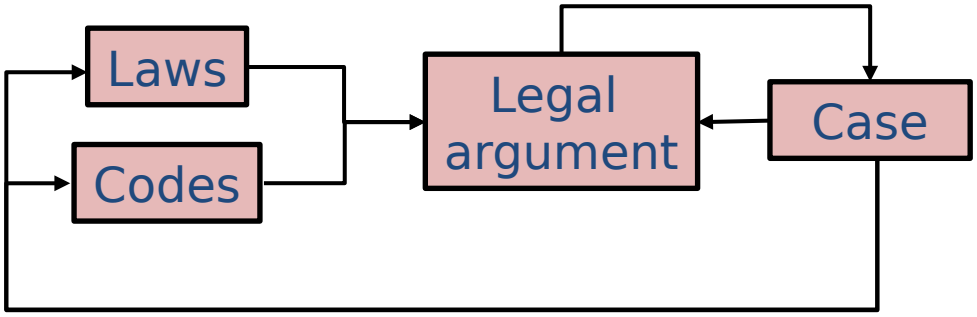
- **Identify which issues are criminal and which are civil**
  - Trespassing
  - Credit card debt
  - Motor racing on a public road
  - Stalking
  - Trolling
  - Not paying council tax
  - Cannibalism
  - Noise pollution

Brief overview of UK Law

- **Identify which issues are criminal and which are civil**
  - Trespassing
  - Credit card debt
  - Motor racing on a public road
  - Stalking
  - Trolling
  - Not paying council tax
  - Cannibalism
  - Noise pollution

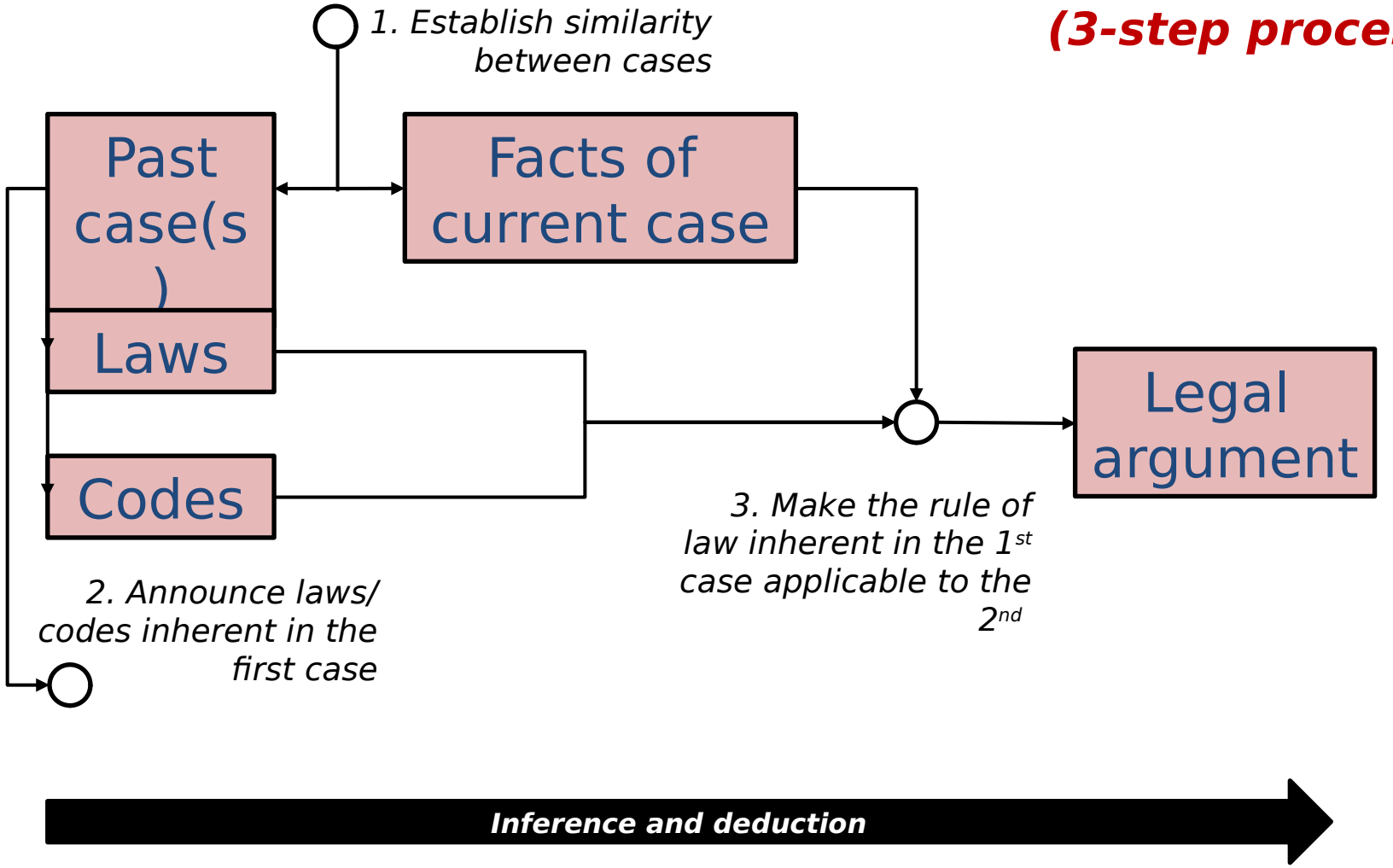
Brief overview of UK Law

- Common Law
  - A legal precedent made by a judge during the course of a case / fluid and interpretive / a judge applies knowledge of legal precedent (prior decisions) and common sense to the facts / cases are individual (unique) / English law works on a common law system / adversarial system / single decided case becomes binding law
- The circular effect of Common Law

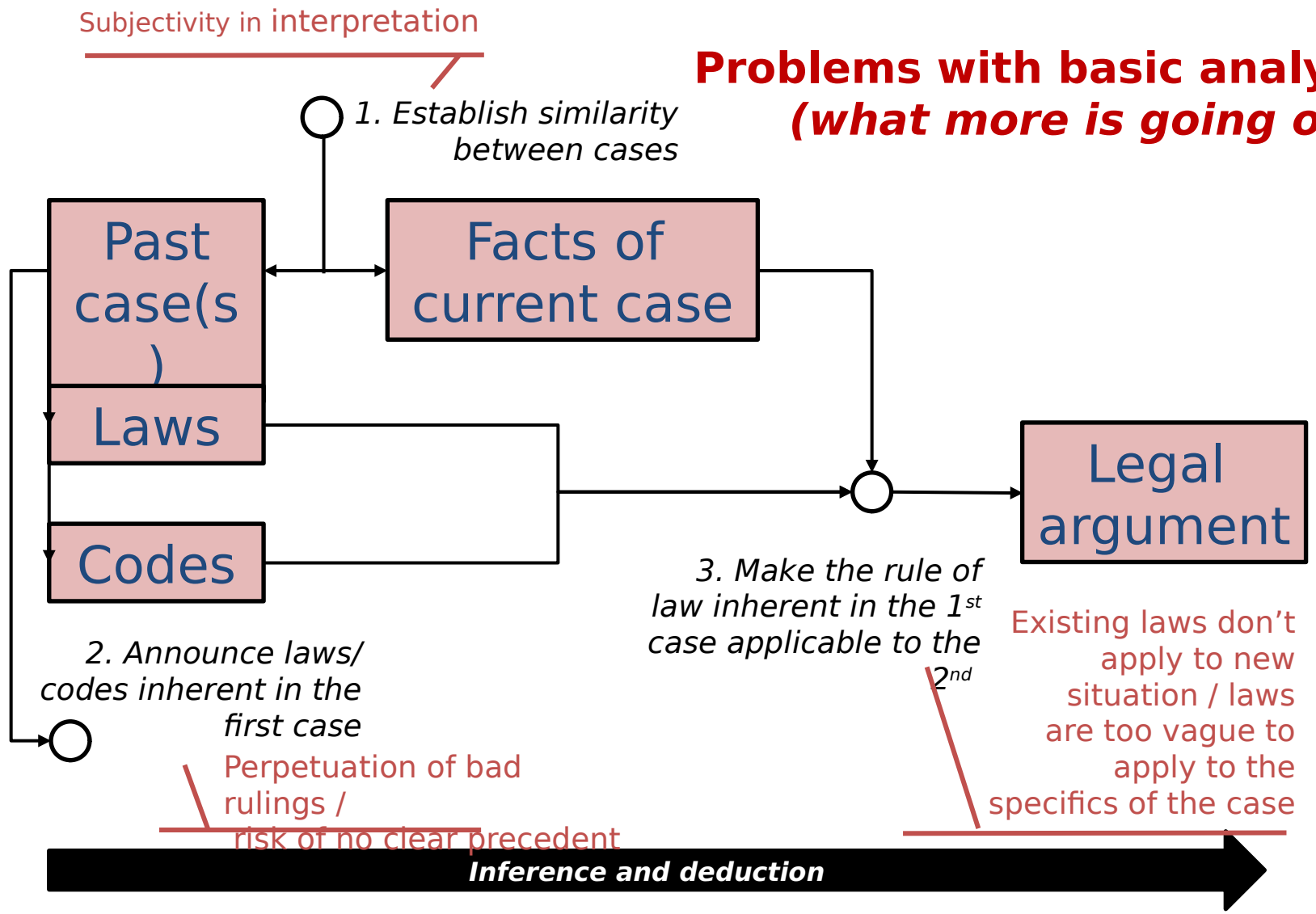


Legal argumentation, reasoning & interpretation

Basic common law structure (3-step process



Legal argumentation, reasoning & interpretation

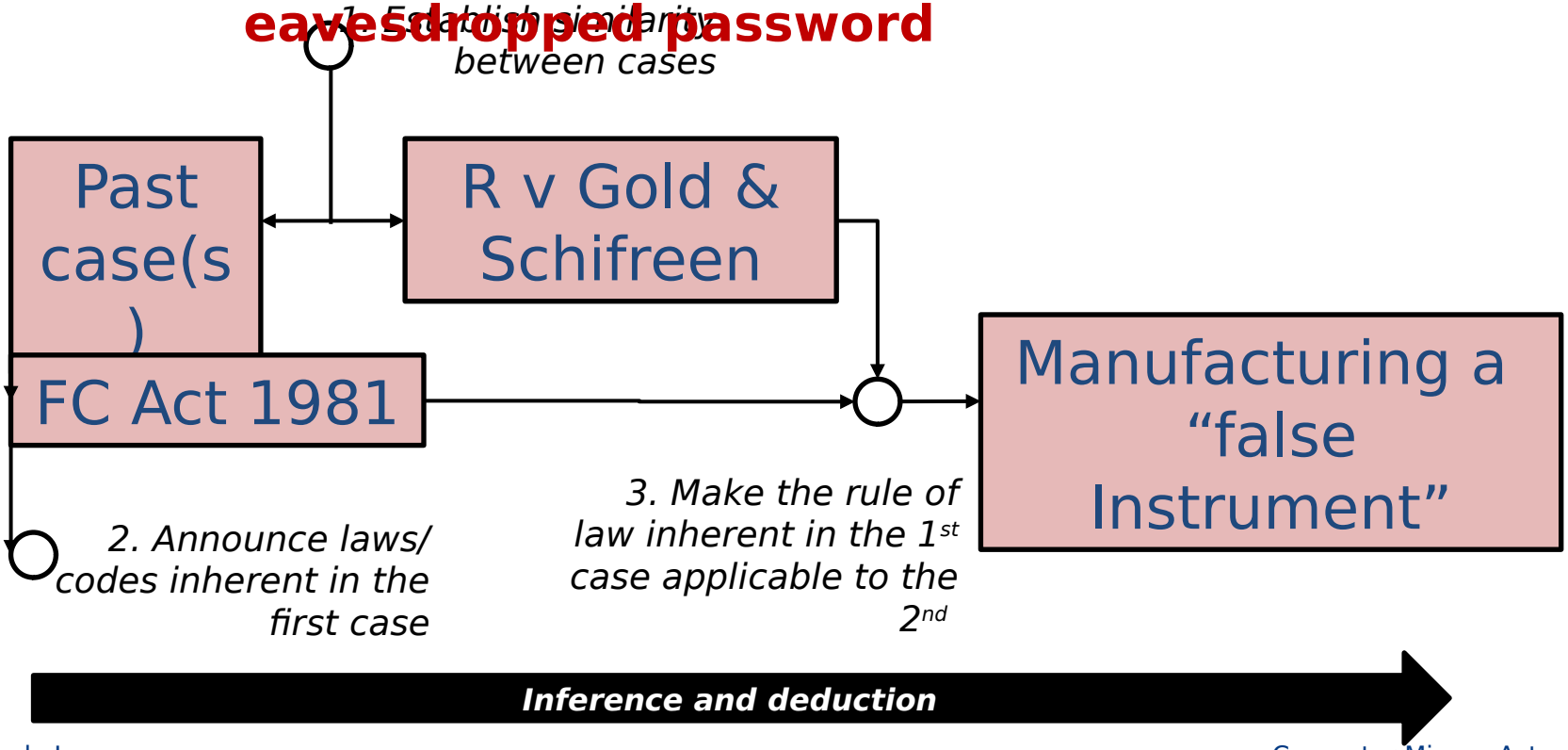


R v Gold & Schifreen

- Robert Schifreen and Stephen Gold, using conventional home computers and modems in late 1984 and early 1985, gained unauthorized access to British Telecom's Prestel interactive *viewdata* service
- While at a trade show, Schifreen, by doing what later became known as shoulder surfing, had observed the password of a Prestel engineer: the username was ‘22222222’ and the password was ‘1234’
- Armed with this information, the pair explored the system, even gaining access to the personal message box of Prince Philip, Duke of Edinburgh.

R v Gold & Schifreen

- **Charged under Forgery and Counterfeiting Act of 1981**
- **Manufacturing a "false instrument"**
- **This referred to the internal condition of BT's equipment following the use of the eavesdropped password**



University of Kent

Summary: Computer Misuse Act

- Section1 - offence is committed as soon as the unauthorised access is attempted
- Section 2 - offence overtakes liability as soon as specific access is made for the criminal purpose
- Section 3 - offence is specifically aimed at those who write and circulate a computer virus or worm, whether on a LAN or across networks

University of Kent

Resources

- Computer Misuse. CPS. https://www.cps.gov.uk/legal-guidance/computer-misuse
- *An Introduction to Legal Reasoning.* Edward Levi. University of Chicago Press
- *Computer Law.* C. Reed and J Angel (eds) 5th edition.
- *Computer Law.* D. Bainbridge. 5th edition.
- Wikipedia 'Computer Misuse Act 1990' [latest acces 19-1-2016 – doesn't spot sneaky "Savings" amendment]