Dealing with computer misuse offences

The UK legal regime and the challenges it entails

The history of the law

- Pre-CMA: Gold and Schifreen gained unauthorised access to Prestel, a large, “subscriber – only” database of valuable commercial services and information

R v Gold & Schifreen

- Gained access to private email accounts (Duke of Edinburgh)
- Hackers sent a message to the Prestel System Manager
- Company to reset all passwords and set a trap for the hackers
- Arrested in 1985 – no idea what to charge them for.

What offence(s), if any, could you charge Gold and Schifreen with?

What did authorities do?

Appeal and chaos

- Defendants found guilty and fined, but appealed
- Argued that 'storage' ("instruments" required that information be stored by mechanical, electronic or other means) cannot be temporary
- The Court of Appeal agreed that the Act was not meant to deal with information held and checked momentarily
- log in details not an "instrument"
- Prosecution was found to be stretching the language of the Act.
- House of Lords appeal by the CPS unsuccessful

Legal system note: The House of Lords was the previous highest UK court. It is now the Supreme Court as of 2009.

I share the view of the Court of Appeal (Criminal Division), as expressed by Lord Lane CJ, that there is no reason to regret the failure of what he aptly described as the Procrustean attempt to force the facts of the present case into the language of an Act not designed to fit them (Lord Brandon).

What now?

- CPS publicly defeated and criticised for prosecuting under the Forgery Act
- Hacking was there and growing
- Need for a new specialised Act
- New offence of unauthorised access to computer data was suggested by the Law Commissions

The CMA 1990

The CMA started with only 3 offences:

- 1. unauthorised access
- 2. aggravated unauthorised access (in order to commit another serious offence)
- 3. unauthorised modification

Section 1 in detail

- A person is guilty of an offence if

a. He causes a computer **to perform any function** with **intent to secure access** to **any program or data** held in **any computer;**

b. The access he intends is **unauthorised**

c. **He knows** at the time when he causes the computer to perform the function that that is the case **(it is unauthorised)**

- NO definition of 'COMPUTER'. **WHY?**
- NO mention of terms like 'HACKING'. WHY?

- Scottish Law Commission: liability for unauthorised access only if intention **to secure a benefit or cause loss**
- Law Commission: mere unauthorised access should suffice **due to the additional costs of hacking…?**
- Law Commission recommendation: Minor offence (3 months imprisonment)
- the Parliament doubled this recommendation
- Police and Justice Act of 2006 increased the maximum penalty to **2 YEARS IMPRISONMENT** - thus extraditable, prosecutable for attempt, incitement, conspiracy

The concept of unauthorised use of authorised access

S17(5)

17. (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

The following text was added by amendment: …references to a program include references to **part** of a program

Consider the Following Circumstances

John returns to a former place of work to make a purchase.

The salesperson, Jane, leaves John alone beside the till terminal.

While Jane is away, John puts a discount code into the terminal to give himself a large discount to his order.

Has John committed any Computer Misuse Offence?

Internal Hackers: So far so simple…

- ***R v Bennett* 1991**: A police SI accessed the PNC to get information on ex-wife and pleaded guilty to s1 Unauthorised access. Fined £150
- ***R v Bonnett* 1995**: A Special Constable looked up a private registration he wanted to buy. Convicted under s.1
- ***R v Begley* 1995**: Officer looked up boyfriend's ex. Charged under s.1

All deemed fairly simple CMA prosecutions as the officers did not have authority to access the particular files. But what if they do….?

Challenge to the CMA: *DPP v Bignell* 19997

- Two married police officers obtained access to data from the PNC in order to identify the owner of a number of motor vehicles (partner of ex-wife of Mr. Bignell)
- The information was sought **for the officers' personal interest - not connected with their duties.**

NB: This is now known as the 'authorized access for unauthorized purpose' defence!

- Upon being uncovered, the defendants were charged under s.1,
- CONVICTED and fined

- On appeal, the Court focused on the literal purpose of the provision:

This was deemed to be: **To protect the integrity of computer systems and not of information stored therein**

- So a person with authorisation to access the computers or data in question **was not violating the CMA** by using their access for an unauthorised purpose
- Result: **no offence under CMA**
- Potential offence under the Data Protection Act 1984 - no prosecution followed
- Lord Astill clarified that internal disciplinary processes *should* still follow.

Heavily Criticised

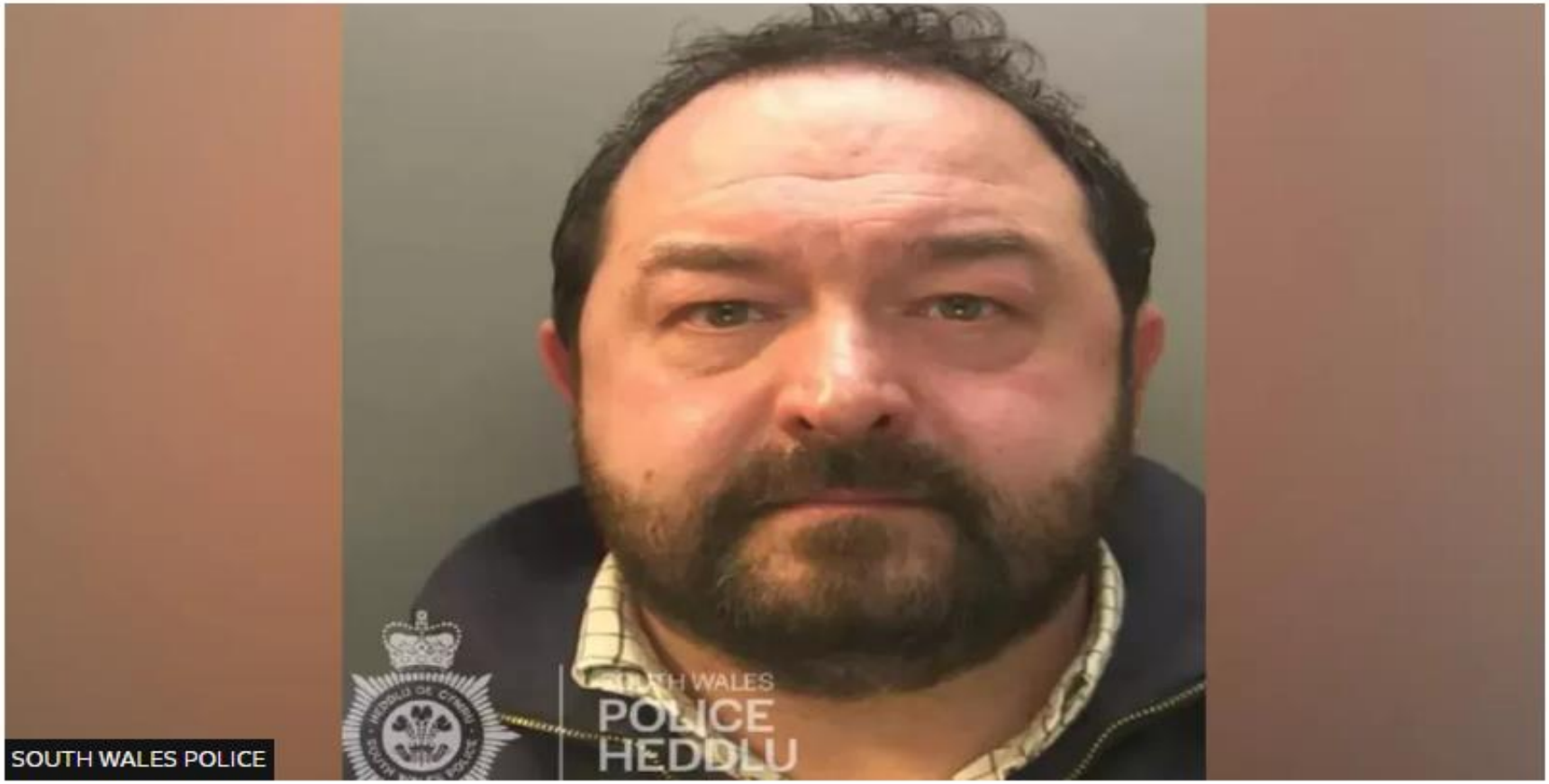
Access vs Control

Specific Data vs. Data of A certain kind/category

South Wales Police: Ex-inspector jailed for computer misuse

23 December 2022

Good news: The law got ‘fixed’. Let’s see how!



The judge told Joseph Jones: "You are someone who's supposed to be upholding the law, and instead you've undermined it"

The Allison [2000] case: The Leading Case

- AmEx employee in the US, Ms Ojomo, gained access to customer credit card accounts and **passed on confidential information to Mr Allison**, resident **in London.**
- The **information was used by Allison to create credit cards**
- Ojomo and Allison arrested
- Allison held on suspicion of conspiracy to secure unauthorised access to the AE computers with intent to commit fraud & forgery (s.2 of CMA) and cause unauthorised modification to the contents of the AE computers.(s.3)

The issue with s.2

(1) A person is guilty of an offence under this section if he commits an offence under s. 1 ('the unauthorised access offence') with intent—

- (a) to commit an offence to which this section applies; or
- (b) to facilitate the commission of such an offence (whether by himself or by any other person).
- The offences it applies are effectively murder **or those for which a person with no CR could be sentenced to 5 years or more**

- It is immaterial whether the further offence **is to be committed on the same occasion** as the unauthorised access
- **or on any future occasion**. (S.2.3)
- A person may be guilty **even though the commission of the further offence is impossible** (S.2.4)
- The maximum sentence for commission of the s.2 offence is **5 years**.
- Rationale: **Bringing forward in time the moment at which a serious criminal offence is committed**

The extradition process

- The US sought to extradite Mr Allison
- Extradition possible only for s. 2 offence - penalties for s.1 were too low to warrant it - NOT ANYMORE AFTER THE POLICE & JUSTICE ACT 2006
- Unauthorised access necessary for proving a s.2 offence
- Court followed Bignell: **the s. 1 offence had not been committed and therefore no s. 2.**

- HoL appeal was successful for prosecution
- Focus on s.17: access is unauthorised if a person:
- (a)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.
- Account had to be taken of **the use to which access was put rather than just type of data accessed**

Coltman (2018) and the Human Rights Question

- Coltman worked for the NHS and accessed a patient file he had no access to.
  - Very straightforward CMA breach.
  - But are there any defences?
- Coltman argues the public interest defence.
  - Judge says he can't.
- Coltman argues that the Human Rights Act 1998 means he has to be allowed it.
  - Final decision: The HRA does NOT mean that the public interest defence has to be read into the CMA.

Computer Damage and External Hacking – S.3 of CMA

- During the 1980s damage to data prosecuted as criminal damage under the **Criminal Damage Act 1971.**
- *In R v. Whiteley* a computer hacker had accessed various computer networks and **deleted a number of files.**
- He was prosecuted and convicted of the offence of criminal damage.
- On appeal he argued there was no **tangible damage to the targeted computers.**

- Rejecting this contention, the Lord Chief Justice ruled that:
- What the Act requires to be proved is that **tangible property has been damaged**
- NOT that the damage itself is tangible.
- **Damage: The particles upon the metal discs had been altered in a way that impaired the value and usefulness of the disc to the owner**
- Most prosecutions use s.3 of CMA now

From modification to impairment

- Initially S.3 related to unauthorised modification
- However **s. 36 of the Police and Justice Act 2006 introduces**:

'UNAUTHORISED ACTS WITH INTENT TO IMPAIR OPERATION OF COMPUTER ETC.'

The offence is meant to

- **regulate the production and distribution of malware**
- **establish a specific digital criminal damage offence and**
- **deal with the problem of DDoS explicitly** (satisfying the Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems)

- **S.3(1)** A person is guilty of an offence if—
- (a) he does any **unauthorised act** in relation to a computer;
- (b) at the time when he does the act **he knows that it is unauthorised**; and
- (c) either subsections 2 or 3 apply.
- **S.3.2**: The intended effect of the unauthorised act must be:
- **to impair** the operation of any computer, computer or reliability of data
- **to prevent or hinder access** to any program or data
- **to enable any of the above.**
- **S. 3. 3** adds **recklessness** as mens rea (PJA 2006 amendment)
- max **10 years on indictment.**

R v Bedworth 1993

- Early cases, e.g., Goulden, Pryce, quite easy. First challenge was Bedworth.
- Bedworth with two others gained access to networks and were charged with ss.1&3
- Accomplices entered guilty pleas – 6 months in prison
- Bedworth pled not guilty to charges of conspiracy to commit ss.1 and 3 offences.
- Defence claimed **addiction to computer use and thus inability to form the necessary intent** (Computer tendency syndrome) –
- Jury acquitted – Heavily criticised outcome – unique case

Other Ambiguities with s3

Bert is a trained security professional and penetration tester.

He sees an appeal by NGO Flood Relief and wants to donate.

He goes to floodrelief.org and notices issues with the website after he doesn't receive a confirmation.

Intending to protect the public, he tests the sites security by altering his privileges and accessing its internals. Bert finds nothing amiss.

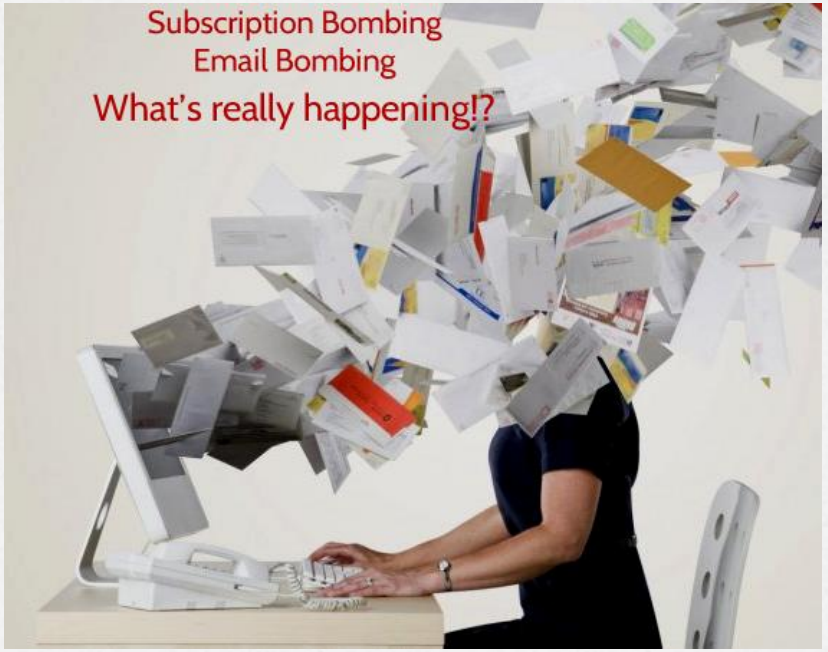
The site admins notice Bert's name on their administrator list and call the authorities.

What should happen to Bert?

DPP v Lennon: The Mail Bombing Case

- Lennon admitted to mail-bombing his employer through a program called **Avalanche**
- **5 million emails** sent - Charges were brought under s. 3 of the CMA (modification at the time)
- The trial judge expressed the view that:
- 1) **s. 3 was criminalising with the sending of malware, but not the sending of emails**
- (2) as servers **were configured to receive emails, each modification occurring by an email sent by Lennon was** authorised

- The prosecutor appealed
- Divisional Court: Consent to receive emails **does not cover emails which are not sent for the purpose of communication with the owner**
- but **for the purpose of interrupting the proper operation and use of his system**
- The respondent was convicted and sentenced to **a 2 month electronic curfew.**



Misuse of devices

- Software can be used in connection with cybercriminal conduct
- A market also exists for trading in user names and passwords and malware
- The Police and Justice Act 2006 added a new section 3A to the Computer Misuse Act

- **S.3A:** A person is guilty of an offence
- (1)if **he makes, adapts, supplies or offers to supply any article intending it to be used to commit, or to assist in the commission** of, an offence under ss 1 or 3.
- (2) if **he supplies or offers to supply any article believing that it is likely** to be used to commit, or to assist in the commission of ss 1 or 3.
- (3) **if he obtains any article with a view to its being supplied for use to commit, or to assist in the commission** of sections 1 or 3 offences
- **article = any program or data held in electronic form**
- Penalty: **2 years max** on indictment.

Any issues with this section?

New Directive 2013/40/EU

- **The Directive led to Serious Crime Act 2015 amending the CMA**
- New offence (s.3ZA) of unauthorised acts that result, either directly or indirectly, in serious damage to the economy, the environment, national security or human welfare, or creates a significant risk of such damage.
- Penalty: up to life for attacks resulting to loss of life, serious illness or injury or serious damage to national security,
- 14 years' imprisonment for attacks causing, or creating a significant risk of, severe economic or environmental damage or social disruption.

Other amendments

- Extend s.3A to include ‘obtain for use’ to cover the event of tools being obtained for personal use to commit offences under ss.1, 3 and 3ZA.
- Extend the existing extra-territorial jurisdiction (s.4): UK nationals committing a CMA offence abroad can be prosecuted solely on the basis of their nationality (act must also be an offence in origin country)
- Calls for a new, more modern Act are common from the industry and academia, but process is slow

Interesting UK cases

- Major cases of Gary Mackinnon and Laurie Love – extradition to the US and the defence based on risk to life due to mental health and being neurodivergent

Precedent: the "forum bar" allows British judges to block extradition if it is not in the interests of justice.

- Julian Assange and his US extradition saga – currently close to being extradited to the US

Cybercrime Convention 2001

- *Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems*
- Article 2 – Illegal access
- Article 3 – Illegal interception
- Article 4 – Data interference
- Article 5 – System interference
- Article 6 – Misuse of devices
- Issues with the Convention?

EU initiatives

- Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA
- Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union
  => replaced by
- Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) GDPR

The suggested UN cybercrime treaty

- Large focus on international cooperation but concerns about human rights
- Finally moving but still issues to resolve after the 2nd ad hoc committee meeting in Vienna
- Some issues: Violation of T&Cs and criminal liability, intent of unlawful hindering of computers (ethical), cyberterrorism and definitions for different countries
- What is the current state of play?

HACKERS CAN TURN YOUR HOME COMPUTER INTO A BOMB

. . . & blow your family to smithereens!

By RANDY JEFFRIES / Weekly World News

WASHINGTON — Right now, computer hackers have the ability to turn your home computer into a bomb and blow you to Kingdom Come — and they can do it anonymously from thousands of miles away!

Experts say the recent "break-ins" that paralyzed the Amazon.com, Buy.com and eBAY websites are tame compared to what will happen in the near future.

Computer expert Arnold Yuberoos, president of the Washington-based consumer group National CyberCrime Prevention Foundation (NCPF), says that as far as computer crime is concerned, we've only seen the tip of the iceberg.

"The criminals who knocked out those three major online businesses are the least of our worries," Yuberoos told *Weekly World News*.

"There are brilliant but unscrupulous hackers out there who have developed technologies that the average person can't even dream of. Even people who are familiar with how computers work have trouble getting their minds around the terrible things that can be done.

"It is already possible for an assassin to send someone an e-mail with an innocent-looking attachment connected to it. When the receiver downloads the attachment, the electrical current and molecular structure of the central processing unit is altered, causing it to blast apart like a large hand grenade.

"As shocking as this is, it shouldn't surprise anyone. It's just the next step in an ever-escalating progression of horrors conceived and instituted by hackers."

Yuberoos points out that these dangerous escapades have already:

- Vandalized FBI and U. S. Army websites.
- Broken into Chinese military networks.
- Come within two digits of cracking an 11-digit Russian security code that would have sent deadly missiles hurtling toward five of America's major cities.

"As dangerous as this technology is right now, it's going to get much scarier," Yuberoos said.

"Soon it will be sold to terrorists cults and fanatical religious fringe groups.

"Instead of blowing up a single plane, these groups will be able to punch into the central computer of a large airline and blow up hundreds of planes at once.

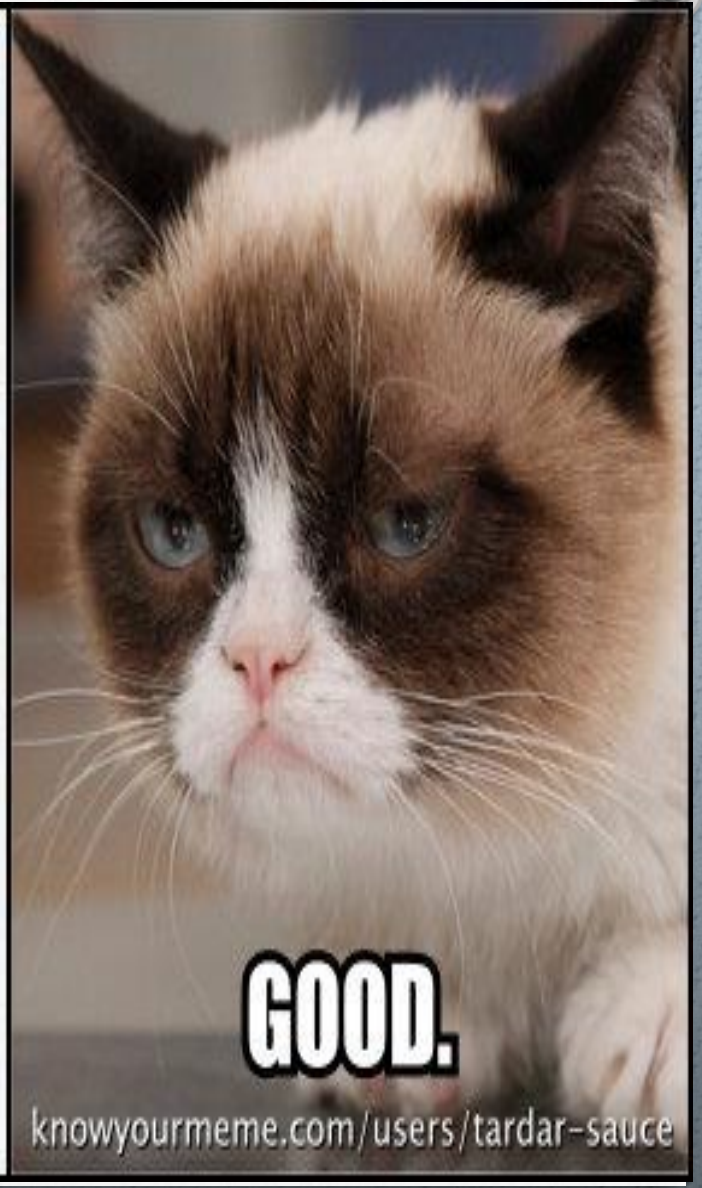
"And worse, this e-mail bomb program will eventually find its way into the hands of anyone who wants it.

"That means anyone who has a quarrel with you, holds a grudge against you or just plain doesn't like your looks, can kill you and never be found out."

Sickos can wreak death and destruction from thousands of miles away!

Arnold Yuberoos

KABOOM! It might not look like it, but an innocent home computer like this one can be turned into a deadly weapon.



The end

Any questions?