Public Affairs Update

February 2023

Malcolm Hutty
Director, Legal & Policy

28th February 2023
LINX118

Agenda

- Data Protection and Digital Information Bill
- Review of the Computer Misuse Act
- Misc

Data Protection and Digital Infrastructure Bill

Data Protection and Digital Information Bill

- Intended to “unlock the value of data” and “secure a pro-growth and trusted data regime”
  - Significantly, to relax aspects of UK GDPR

- Some key changes
  - Narrows definition of “personal data” slightly
  - Restrictions on automated decision-making limited to special category data
    - But transparency and contestability requirements remain
  - Purpose limitation for processing restated
  - Adds a set of recognised legitimate interests that automatically qualify
  - Subject access requests exempted where “vexatious or excessive”
  - Data Protection Officer replaced with Senior Responsible Individual
    - The DPO had to be independent of management; the SRI is supposed to be a part of the senior management
  - Some simplification of record-keeping of processing and easing of requirements for data protection impact assessments
  - Information Commission(er) to become more like other regulators

- Broadens the use of cookies without requiring opt-in user consent
  - Functional elements of website, service or app
  - To maintain user preferences
  - To enable software updates for security of a user device

- New duty for network operators (PECS) to notify the Information Commissioner of unlawful direct marketing using their service
  - Notification required for **every** time PECS has reasonable grounds to suspect a breach of the regulations (PECR) by one of their users
  - **FIXED PENALTY REGIME** for failure to notify (£1000)

Computer Misuse Act consultation

Computer Misuse Act 1990

- A simple Act with 18 sections.
- Originally three offences:
  - s.1 Unauthorised access to computer material
  - s.2 Unauthorised access with intent to commit or facilitate commission of future offences
  - s.3 Unauthorised modification of computer material
- Later additions
  - s.3ZA Unauthorised acts causing or creating risk of serious damage (Serious Crime Act 2015)
  - s.3A Making, supplying or obtaining articles for use in offence under s.1., s.3, or s.3ZA
- The rest is jurisdiction and miscellaneous
  - *No new police powers*

2023 Consultation (1)

- Domain name and IP address ‘takedown’
  - New LE power to take down domain names
  - New LE power to take over domain names i.e. direct to an address used by LEA.
  - Power to prevent domain registry creating a domain name
    - For where LE become aware of a domain generation algorithm, e.g. included in botnet code.

- The above is more straightforward for domain names, less so when applied to IP addresses.
  - Includes IP address ~~blackholing~~ sink-holing.
  - Would include a requirement for network operators to receive traffic intended for a targeted IP address on their network, and tunnel it back to an address used by an LEA.

2023 Consultation (2)

- New data preservation power
  - To allow an LEA to require preservation of 'specified computer data' by 'a person in control of such data'
  - Does not include power to acquire it
  - Home Office refers to ninety day time limit on preservation requirement in the Budapest Convention on Cybercrime, says this would be reasonable.

- New offence of copying data obtained through a Computer Misuse Act offence.
  - Home Office professes to be undecided on this: "we would like to consider"
  - In what circumstances would this be problematic? Are exceptions needed?

2023 Consultation (3)

- The current law has a scattering of extra-territorial provisions, applying the existing offences
  - To those things when done in the UK, by anyone
  - To those things done by UK nationals, anywhere in the world, if illegal there
  - To those things done when to any computer or data in the UK, regardless of by whom or from where
  - To those things done using computers in the UK, regardless of by whom or to what
- …but not each of these rules applies to each offence.

- Government is consulting on unifying these into a single extra-territoriality rule.

2023 Consultation (4)

- Should new explicit defences be introduced to protect “legitimate cyber security activity”?

- Government does not want to create a right to “hack back”

Misc

Online Safety Bill

- Now in the Lords
- Personal liability for senior managers back on the table
- Potential for extension to suppress other kinds of lawful content (e.g. "health misinformation") being explored by opposition parties
- Powers that can be used to compromise or ban end-to-end encryption in user-to-user communications services
- Concern about Minister "meddling" in Ofcom via directions
  - But CSEA and terrorism Codes only directable for reason of public safety or national security, not to increase freedom of expression or proportionality

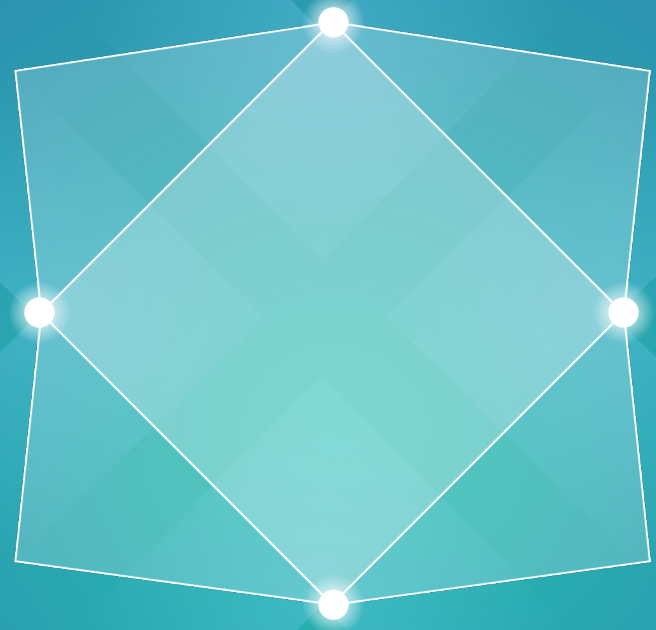
Artificial Intelligence

- Copyrightability of AI output
  - "Zarya of the the dawn", a graphic novel significantly created by AI art package Midjourney
  - US Copyright Office held that copyright subsists in those portions created and assembled by the human author, but not in those portions created by Midjourney

- Liability for AI output
  - People are having fun trying to get ChatGPT and Microsoft Bing Chat to say things it shouldn't.
  - Prompt-based programming and "jailbreaking"
  - Who is liable for AI output?

linx

Thank you. Questions?



malcolm@linx.net

linkedin.com/company/linx/

facebook.com/LondonInternetExchange/

twitter.com/linx_network

youtube.com/user/LINXnetwork