

# Trade secrets and digital data: Panel 4

**WIPO Trade Secret Symposium, 23 May 2022**

Professor Tanya Aplin, Dickson Poon School of Law, King's  
College London

# Thoughts on Japanese model of "shared data with limited access"

---

- Scheme applies to *any* data (except secret or open data) that is shared; therefore, provides **far-reaching protection** for data
- Any such scheme would cause **difficulties** with coordinating data access and data use rights
- Relatively new scheme whose positive impact on data sharing is, as yet, **unproven**
- Need to be **wary of legal transplantation** – right was developed within a specific legal context

# What about trade secrets protection?

---

- **Trade secret protection is not a data-economy specific form of regulation**, but may be useful because of breadth of the definition of trade secret and flexible, unfair competition-like form of protection
- Mandated by Art 39 TRIPs (and in the EU by Trade Secrets Directive 2016/943 (TSD)) so **available in multiple jurisdictions**
- **Unregistered** form of protection (so no *ex ante* assessment)
- Limited in **duration** only by the secrecy of the information

# Can data qualify as a trade secret?

---

- **Individual data** – unlikely to be useful or meaningful in isolation (not semantic information) and thus will lack commercial value
- **Individual level datasets** (e.g. generated from a connected device) – may not have commercial value since it does not necessarily affect the competitive advantage of the manufacturer of the device (except where data relates to technical functioning of the device)
- **Aggregated datasets** – well-developed markets for this data but need to ensure there is secrecy and commercial value due to secrecy
- **Training data for AI** – where drawn from public sources then not protected; investment in labelling or cleaning creates commercial value but this does not mean there is a commercial value due to secrecy
- **Output of AI training technique** – this might qualify

# Is the scope of protection appropriate?

---

- Protection is **unfair competition** rather than property rights, and prohibits **unlawful acquisition** by conduct contrary to honest commercial practices, and **unlawful use or disclosure** following on from unlawful acquisition or a breach of contractual or other duty not to disclose or use
- **Extends to third parties** where at time of acquisition, use or disclosure third party has knowledge that the trade secret was obtained from another person who was unlawfully using or disclosing the trade secret
- In the EU, also **extends to commercially dealing in infringing goods** – i.e. goods whose “design, characteristics, functioning, manufacturing process or marketing significantly benefits from trade secrets unlawfully acquired, used or disclosed” - **broad reach** that may apply to digital products - although note the knowledge requirement

# Do trade secret limitations suit the data economy?

---

- **Limitations**, e.g. for reverse engineering and in the public interest in EU TSD have **limited relevance to the data economy**
- Query whether **reverse engineering** digital products will give rise to the data that is being collected, processed or on which it has been trained. Note also (in the EU) the role of contractual override where the product is lawfully in the possession of the acquirer of information
- **Public interest** limitation is directed at revealing misconduct, wrongdoing or illegality, as opposed to promoting data sharing
- **Freedom of expression** limitation is also linked to whistleblowing, as opposed to data sharing to promote the data economy