



# Data Innovation, Complementarity and Firm Growth: A Discussion

Enisse Kharroubi

BIS

**Workshop on Artificial Intelligence in Finance**  
**IESE Business School, Barcelona**

March 20, 2025

---

The views expressed here are those of the authors and do not necessarily represent the views of the BIS.

## Short Summary

- ▶ The paper introduces the notion of innovation complementarity at the firm level and provides an empirical and theoretical analysis of its implications.
- ▶ The paper does so:
  - ▶ Empirically, by constructing a measure of innovation complementarity and looking at the impact of the introduction of the Data Breach Notification Law (DBNL) regulation on high vs. low complementarity firms .
  - ▶ Analytically, by building a model where firms are heterogeneous in their ability to invest in data security, as well as in the benefits they can reap from these investments.
- ▶ The notion of innovation complementarity is the idea that the benefits of investments/innovations in data security extend well beyond their initial purpose and can for instance, foster innovations outside the area of data security.

# Main results of the paper

The main results of the paper as follows:

1. Empirically: the introduction of the DBNL regulation has benefited disproportionately to high-complementarity firms. Such firms increase innovation, become more profitable and are able to hold a larger market share.
2. Analytically: When data security becomes more important, high-complementarity firms invest more in data security, which provides them with further benefits in terms of productivity. The productivity gap between high- and low-complementarity firms goes up

# Comment 1: The empirical measure of complementarity

- ▶ The construction of the complementarity measure rests of some disputable choices:
  - ▶ The threshold for classifying data-security v. other innovations (10%) is rather low.
  - ▶ The complementarity is estimated considering the involvement of *current* data-security innovators in *subsequent* non-data-security innovations. This is restrictive.
  - ▶ Highly innovative firms have strong incentives to invest and innovate subsequently in data security. They may also do both at the same time.
  - ▶ The threshold (75th percentile) defining high complementarity firms being sticky, their fraction is increasing over time. This seems more an artefact than a genuine empirical development.

# Comment 1: The empirical measure of complementarity

- ▶ The construction of the complementarity measure rests of some disputable choices:
  - ▶ How big are in-house vs. external data security innovations, acquired ready on the shelves?
    - ▶ Are firms doing most of it on their own?
    - ▶ Data security is very technical. Specialisation whereby data-security firms sell data-security products to other firms would make sense.
    - ▶ How much of data-sec innovation is conducted outside the "data-sec" sector?
  - ▶ The paper should provide points of comparison to evaluate the complementarity measure:
    - ▶ Are high-complementarity firms just highly innovative firms, or is there something else?
    - ▶ Does high vs. low complementarity correlate with breakthrough vs. incremental innovations?

## Comment 2: The roll-out and impact of DBNL

- ▶ The paper leverages the staggered introduction of DBNL across US states to estimate its impact on high- vs. low-compl. firms
  - ▶ States likely chose to apply DBNL regulations earlier where data security was a big issue for firms  $\Rightarrow$  not surprising CA was first.
  - ▶ Timing of implementation was not random vis-a-vis the presence or the acuity of data security.
  - ▶ Implementing DBNL obviously raises the cost of data breaches and raises the value of data security.
  - ▶ Firms should therefore innovate but more importantly *invest* more in data-security  $\Rightarrow$  focus on innovation is too narrow
  - ▶ A lot may have happened that is *not* about innovation.
  - ▶ The evidence on profitability going by more for high compl. firms is interesting but unlikely to reflect innovation decisions, which take time to translate into profits.
  - ▶ Rather ability to make more money out of data-sec products looks like a more compelling possibility.

## Comments 3 The model

- ▶ The value of profits for high-and low-compl. firms is:

$$V_h(a_{i,t}, \tau_t, s_t) = \bar{A}e^{b(\tau_t - \iota s_t)} - (a_{i,t} - \theta_{i,t} - \epsilon_{a,i,t})^2 - \tau_t + p_t s_t$$

$$V_l(a_{i,t}, d_t) = \bar{A} - (a_{i,t} - \theta_{i,t} - \epsilon_{a,i,t})^2 - p_t d_t$$

- ▶ Investments in data-sec.  $\tau_t$  and supply and demand for data-sec. products  $s_t$  and  $d_t$  improve the precision of the signal on  $\theta$ :

$$\Omega_{h,t+1} = [\rho^2(\Omega_{h,t} + \sigma^2)^{-1} + \sigma_\theta^2]^{-1} + [1 - \nu e^{-(\tau_t - \iota s_t)}]z\sigma_\epsilon^{-2}$$

$$\Omega_{l,t+1} = [\rho^2(\Omega_{l,t} + \sigma^2)^{-1} + \sigma_\theta^2]^{-1} + [1 - \nu e^{-d_t}]z\sigma_\epsilon^{-2}$$

- ▶ Data-sec. innovation is a dual benefit activity for high compl. firms: it improves both productivity and signal precision  $\Rightarrow$  The model's properties are hard wired into this assumption.
- ▶ In reality, firms choose between these different activities. A sketch of complementarity:
  - ▶ Strong innovation increases the need to secure data
  - ▶ Strong data security reduces risks of innovation being leapfrogged/captured by competitors