Data As a Sinister Weapon

*Here, **Lisa Burton**, GLL Ambassador and Chief Executive Officer of Legal Data Workspace, reflects on the negative imact data can have when being used as a weapon and offers key tips on managing data as a reliable reportable asset. Read the full article on our website here.*

As frequently mentioned in this column, **data is both an asset and a risk. Unfortunately, it is a weapon too.** For example, Ukraine suggests that "Russia continues to receive almost instantaneous meteorological data from foreign governments, which some experts say could be used to plot a chemical or biological attack in Ukraine." Meteorological data is apparently vital in chemical warfare as the perpetrator cannot risk 'blow back' of chemicals through moving weather systems. Sinister stuff.

Another example of data being used as a weapon is racism within Football. The continued racist abuse that flows through Facebook, Twitter and Instagram, are from trolls traced back to non-Westernised countries. Even so, Instagram was the first social media to blink as the pressure builds. The platform does not use technology to proactively detect content within private messages, but it has announced new measures, including removing abusive accounts, in a bid to reduce the abuse people get in direct messages.

As Western individuals, we are all well aware that our buying preferences are continuously profiled evidenced by conversations about trainers that then miraculously appear as adverts on our open laptop screens. Most of us accept this is part of living in a digital age but there are some very dark implications of this, especially for our future generations. In being 'fed' data through personal preferences, the risk is we lose our ability to make informed choices. **There is so much digital information how do we know what to trust and what not to?**

As someone who identifies as Jewish, it is not lost on me that the first significant regulatory policy enhancement to E.U. data protection regulations in more than 20 years, the GDPR requires companies to ask consumers whether they can collect their data, answer promptly if asked what it'll be used for and disclose significant data breaches within 72 hours. As we all know, failure to fully comply with the law could result in hefty fines and consequences for a business.

The seriousness of the penalties reflects a European approach to privacy that can be traced back, in large part, to German history — and to specific experiences with personal data being used for the most heinous purposes.

As the Nazi regime rose to power, state control of businesses brought with it state control of information technology. Regulation continues to expand its reach around information technology and data, especially in already highly regulated markets. DORA, the Digital Operational Resilience Act, is draft legislation designed to improve the cybersecurity and operational resiliency of the financial services sector. While DORA is still working its way through the legislative process, it is expected to be approved in 2022. It will expressly focus on ICT companies that serve their financial services clients.

This will have a vast impact on MSPs providing Cloud and Managed Services encompassing evergreen platforms such as M365 and Google Business because although regulatory compliance must evolve with the business, a continually updated platform, means that functionality will evolve too. Regulatory compliance and tech stacks must be aligned to protect businesses with strong operationally living policies that can be measured and reported on a Data Balance Sheet.

In Summary, data as an asset and a risk to a business is one thing. Data used as a weapon is on the increase and as we are already experiencing in the Russian Ukraine war, it can be deadly. In a digitised global community, businesses must protect their employees, customers and partner communities to preserve the core fundamental principle of human rights and democracy.

At Legal Data Workspace, we are proud to support charities by providing free Data Protection Awareness Sessions and Training for their Boards and teams handling data.

I wanted to provide some top tips on one element that our free training encapsulates. For a Charity, seeing data as an asset and being able to put a figure on its value can be very empowering to attract further corporate support through donations, supply chains and their volunteering networks.

Our messaging is clear that companies today are deriving competitive advantage, intellectual property gains and even data monetisation from their data. For those companies that are actively monetising their data by reselling it to others, there is likely a very tangible way of measuring profits from the effort.

For the majority of companies that use data for competitive or marketing advantage, there's one way to calculate if the use of data is what's responsible for a certain profit number, whether that number comes from an increase in sales or market capture. They have to compare the results of their data-driven campaigns to campaigns that did not use this data.

Here are 3 key tips to help with managing data as a reliable, reportable asset on the balance sheet:

1. OPERATIONAL EXPENSE

If data is to be considered as an asset on a balance sheet, there must be a corresponding cost for acquiring or building this asset. Organisations have to value the hours spent on collecting, refining and enriching their data, as well as the personnel recruiting costs, storage and computing costs, facility costs and any other cost factors that go into data asset development. In some cases, organisations are already doing this with their return on investment (ROI) formulas where they track the costs going into data development and put it against the cost of acquiring the data as an asset–but this practice is largely done on a per project and not on a corporate-wide basis. This is where CXOs need to get to work.

2. DATA DEPRECIATION

As data ages, it loses its relevance and its value. Formulas will need be devised to depreciate data over the period of time that it ages (e.g., depreciation taken over three years, five years, etc.). To determine the correct depreciation cycles, regulators and CFOs will need to work together with CIOs to determine what normal lifespans for data are–and then factor in a viable depreciation formula against these lifespans.

3. DATA WASTELANDS

Enterprises have pockets of useless data. It might be data that dates back over ten years that is no longer relevant to what the corporation does, or data that has been routinely stored or backed up, that is temporary or that no one understands. There is an ongoing cost to maintaining these data wastelands and there will be time when the best practice is to purge them. If they are sitting on corporate balance sheets, they will also have to be expensed. The best move here for CXOs is to only admit data that has proven worth to the corporate balance sheet so that charge offs can be minimised.

"There's this misperception that it's a protectionist response, but the roots are much deeper. We trace them back to World War II and the atrocities of the Nazis, who systematically abused private data to identify Jews and other minority groups,"

***Anu Bradford,** Professor, Columbia Law School*