When Data Protection Is a Hindrance Rather Than a Facilitator

The comedy catchphrase "computer says no," coined by the UK television show *Little Britain*,[1] has become embedded in popular culture and now often serves as a simplified excuse for the failure to provide good customer service. However, there has been a sea change in the way data are organized and managed in enterprise environments—a shift that has been a key factor in the decline of effective customer service across many industries.

At the heart of this problem is the fact that the IT sector has not been able to deliver and utilize effective data management and governance tools. In the era of big data and the digital transformation that surrounds it, many users are still wedded to the one data store mindset, trying to find imaginary needles in haystacks with vaporware artificial intelligence (AI). Organizations need tools developed with the understanding that data components in a supply chain are both physically balkanized and have no consistent metadata to be used to discover and address them, let alone work out what least privilege is needed to access them securely.

As it stands, current consumer privacy protection laws, such as the EU General Data Protection Regulation (GDPR) and the US State of California Consumer Privacy Act (CCPA), have been codified in such a way that they actively detract from the customer service experience. The stronger security measures dictated by previous security breaches and regulations have led to an environment wherein all personal data are firmly secured behind these laws, even when the flow of these data would be wholly advantageous to the customer and the organization alike. As a result, data protection has become a catch-all excuse for poor service—a problem that can only be solved with a mixture of transparency (both governmental and organizational) and regulatory initiatives.

Current Issues With Data Protection

Technology has been a major catalyst for the degradation in customer service. The era that began with highly centralized systems based on a mainframe transitioned to the client/server era, when personal computer (PC) file server platforms such as Novell Netware rose in popularity, before evolving into the present era dominated by mobile and cloud platforms.

Data platforms have become heavily fortified through multiple forms of authentication and authorization, in part due to malware events such as the Slammer campaign in 2003, which affected 75,000 servers in 10 minutes and resulted in USD$1.2 billion in financial damage.[2] More recent forms of extortion have impacted the UK National Health Service (NHS), such as the WannaCry attack in 2018, which cost the NHS £92 million after 19,000 appointments were cancelled.[3] Because of major attacks such as these,

RUPERT BROWN

Has been part of the C-suite for many decades, developing, implementing and managing enterprise and trading risk technology with some of the largest and most influential global financial institutions, including MarkLogic, UBS, Merrill Lynch and Thomson Reuters. These institutions have benefited from Brown's vision, experience and ability to deliver enterprisewide change. Having seen the shortcomings of the first generation of RegTech solutions, he set about creating a better solution that incorporated the all-important legal perspective—the result is Evidology Systems.

technology users have become familiar with text message validations, activation codes and two-factor authentication—all of which have been put in place over the past decade. However, this solution can sometimes be a hindrance to users trying to get into an account that requires not one, but often many extra steps to gain access.

Large enterprises have also restructured themselves; sometimes due to regulatory imperatives such as the ringfencing of retail and investment banking activities after the 2008 global financial crisis[4] and, more recently, the impact of Brexit forcing UK organizations to have EU-based subsidiaries to reduce export controls.[5] Although these restructuring activities usually and correctly impose some hard boundaries between legal entities (e.g., banks are now split into retail and investment bank legal entities with no reporting lines across boundaries) the brand identity of the enterprise usually remains intact, which creates a false perception of unified and seamless customer service. This problem is often exacerbated by similar customer-facing segmentation between business and operating utility functions and basic retail consumer interactions. Inevitably, this leads to frustration as customers who think they are dealing with a unified organization instead find that their queries are being addressed by completely separate entities.

Consumers are often blamed for the data privacy issues faced by retail organizations; however, issues may arise from the wholesale side of the business, or from the contractors used to deliver the product or physical service. While some retailers may try to argue that family members sharing passwords without proper authorization is the largest current data privacy issue, the reality is that a majority of issues, in fact, stem from the improper sharing of data between retailers and the wholesale suppliers or distributors on which they rely. Information sharing between retailers and suppliers can lead to increased profits, but done incorrectly, it can quickly create risk around a consumer's data privacy.

GDPR has imposed a safety-first approach on these interdependent supply chains—an approach that was then incorporated into other laws, including the CCPA. This type of regulation makes it far too easy to prevent necessary and timely information sharing without explicit up-front contractual specifications, which lag rather than lead the core business interaction specifications. This is exemplified in the US-based *Dilbert* syndicated cartoon strip, which has a character named Mordac, The Preventer of IT Services.[6]

In the event of a mistake, the mere mention of GDPR to customer-facing employees can engender the fear of liability. It is reasonable to presume that it has been used as cover for a round of redundancies to eliminate the lower-performance quartiles.

Possible Solutions

Common sense needs to prevail, and people must be empowered to champion the customer cause. Although the prime drivers of GPDR sought to protect an individual's personal data, they failed to analyze and address the common scenarios that require data interchange and the need for short-term administrative privileges. A common example of this is the confusion that can occur when an organization pays for an affiliation to a professional body for its staff. The three-way link between the organization, individual and the professional body can lead to trouble if circumstances change on any side as individuals, not their parent organizations, must grant access to their data. These problems typically are worked around through disjointed processes and formal software application programming interfaces (APIs) but, occasionally, organizational restructurings allow for them to get swept under the rug entirely.

In the event of a mistake, the mere mention of GDPR to customer-facing employees can engender the fear of liability.

Much more clarity is needed as to what is truly personal. If personally identifiable information (PII) is available on a public register such as an electoral roll (a list of people who are qualified to vote for certain elections in a particular jurisdiction) or Companies House (the UK's register of companies), then those data elements are outside the scope of legal protection. However, there are many reasons that prevent this information's use. In GDPR, for example, there is no definitive provision that determines whether private information held on public registers is

exempt. Because of the lack of boundaries placed on GDPR, it is nearly impossible to definitively state what qualifies as public information.

The UK Information Commissioner's Office (ICO) sends a letter annually to all organizations registered at Companies House that have not previously paid their annual fee to be a data controller. The presumption of the letter is that all organizations are data controllers and use personal information in their daily business. This does not take into account the fact that many organizations are purely business-to-business (B2B) or only make monetary business-to-customer (B2C) transactions and do not store any customer data. The letter does not attempt to explain this and suggests it is best to pay anyway rather than properly explaining the requirements. Because of this, the letter in itself is highly misleading.

Along with technology and legislative impetus, there is also a need for regulatory initiatives to untangle this Gordian Knot.[7] Regulators must change from a culture of balancing risk to more interventionist problem solving, but they will need both sharper teeth to impose fines for bad behavior and budgets to compete for talent.

Recently in the United Kingdom, the Competition and Markets Authority (CMA) owned the open banking APIs, but the ICO owned privacy matters around the content used in those APIs.[8] It was a recipe for failure, especially when none of the core representatives involved had ever written an API or operated a platform that delivers a service using one.

UK economic policy is often criticized for trying to run businesses on a shoestring budget while also increasing layers of outsourcing rather than relying on automation. If the problems could be fixed in the data supply chain (which is as rife with problems as physical supply chains), then progress can be made. Unfortunately, there is little evidence of any appetite to do this beyond the post-Brexit claim that UK-based organizations are finally able to cut the red tape of EU regulations.

In practice, the only effective remedy is to withhold payments for poor service due to claims of data privacy, a strategy that relies on an organization's biggest motivating factor—its profits—to get things fixed. It is worthwhile to challenge the drudge in the call center to get legal counsel on the phone when an organization claims data privacy issues. This is especially true when it can be demonstrated that the provider has been given enough pointers to resolve matters through a simple search of its systems, rather than being handed an easy answer or given the free gift of a direct debit.

Regulators must change from a culture of balancing risk to more interventionist problem solving, but they will need both sharper teeth to impose fines for bad behavior and budgets to compete for talent.

Conclusion

Since GDPR's introduction in 2018, the landscape of data protection has invariably shifted toward a prohibitory environment wherein all data are kept under lock and key, even when data sharing would benefit all involved parties. Instead of providing consumer protection, GDPR and similar laws have, at times, become all-encompassing excuses for poor customer service. Across the board, these regulations need to establish clear protocols for data sharing within and across organizations while also increasing and reinforcing the penalties for those who improperly utilize customer data to combat systemic issues.

Data protection has transformed itself, in the majority of use cases, from a necessity into a cynical afterthought that is all too easy to use as a fallacious excuse for not meeting service obligations. It is time to end this charade.

Endnotes

1 *Little Britain*, BBC, United Kingdom, 2003
2 Leman, J.; "Eleven Malware Attacks That Nearly Wrecked the Internet," *Popular Mechanics*, 31 October 2019, *https://www.popularmechanics.com/technology/security/g29625471/history-of-malware-attacks/?slide=1*

LOOKING FOR MORE?

- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

3 National Health Executive, "WannaCry Cyber-Attack Cost the NHS £92m After 19,000 Appointments Were Cancelled," 12 October 2018, *https://www.nationalhealthexecutive.com/articles/wannacry-cyber-attack-cost-nhs-ps92m-after-19000-appointments-were-cancelled*
4 Britton, K.; L. Dawkes; S. Debbage; T. Idris; "Ring-Fencing: What Is It and How Will It Affect Banks and Their Customers?" *Bank of England Quarterly Bulletin*, 2016, *https://www.bankofengland.co.uk/-/media/boe/files/quarterly-bulletin/2016/ring-fencing-what-is-it-and-how-will-it-affect-banks-and-their-customers.pdf*
5 Her Majesty's Treasury, "Ring-Fenced Bodies (Amendment) (EU Exit) Regulations 2018: Explanatory Information," United Kingdom, 29 October 2019, *https://www.gov.uk/government/publications/draft-ring-fenced-bodies-amendment-eu-exit-regulations-2018/ring-fenced-bodies-amendment-eu-exit-regulations-2018-explanatory-information*
6 Adams, S.; *Dilbert*, Comic Strip, 5 June 2000, *https://dilbert.com/search_results?terms=preventer+of+information+services*
7 Merriam-Webster Dictionary, "Gordian Knot," *https://www.merriam-webster.com/dictionary/Gordian%20knot#:~:text=Definition%20of%20Gordian%20knot,the%20Great%20with%20his%20sword*
8 Shah, D.; "CMA Letter to Barclays About 13 Breaches of the Retail Banking Order," Competition and Markets Authority, United Kingdom, 21 March 2022, *https://www.gov.uk/government/publications/cma-letter-to-barclays-about-13-breaches-of-the-retail-banking-order*