CEJ
COMPLIANCE
ELLIANCE
JOURNAL

THE UNCONSCIOUS CONSCIENCE OF DIGITAL TRANSFORMATION: THE CHIEF COMPLIANCE OFFICER?

A Thought Piece

Michele DeStefano, Isabel Parker & Giorgia Vulcano

AUTHORS

Michele DeStefano is a Professor of Law and the Larry Hoffman Greenberg Traurig Business of Law Chair at the University of Miami School of Law, a Program Chair and an Affiliated Faculty member at the Harvard Law School Executive Education Program, and an Affiliated Faculty member at IE Law School. She is also the Founder of LawWithoutWalls, Founder and Content Curator of the Compliance Elliance Journal, and a Co-creator and Chief Faculty Advisor of the Digital Legal Exchange.

Isabel Parker is a Partner in Legal Management Consulting at Deloitte Legal and also a Faculty Advisor at the Digital Legal Exchange, a non-executive Board Member at the College of Legal Practice. She has extensive experience in the legal market and was formerly an associate and later the Chief Innovation Officer at Freshfields Bruckhaus Deringer.

Giorgia Vulcano is a US/European lawyer with a background in human rights and international law. She has worked in both global organisations and digital start-ups across Latin American and Europe, helping cross-functional and cross-cultural teams define the legal path to develop and innovate in a sustainable and human centered way. Currently, she serves as legal subject matter expert and counselor on digital ethics, innovation and data protection laws. She is a Faculty member of the Digital Legal Exchange, Board Member of W@Privacy and Education Advisory Board Member of the International Association of Privacy Professionals (IAPP).

The authors would like to thank our interviewees and participants of the Digital Legal Exchange Salon Event in February 2023 for their thoughts and contributions.

TABLE OF CONTENTS

I. INTRODUCTION

Corporations around the globe are embracing Digital Transformation ("DT") to enhance competitiveness i.e., streamline operations, strengthen relationships with customers, and increase revenue.[1]

In this dynamic digital world, where data and algorithms are increasingly leveraged both for decision-making and to achieve economic and social objectives, a relevant digital transformation requires corporations to, not only onboard new technologies and ways of working, but also to address how they will be using tech in a responsible, ethical, customer/consumer-centric, and sustainable way.[2] Necessarily, functions that directly impact the bottom line (like Sales, R&D, Supply Chain) are deeply engaged in these DT efforts.[3] The question is what role is and should Compliance be playing in these DT efforts.

This thought piece focuses on the evolving role of the Compliance function in this rapidly developing ecosystem, analyzing what role does – and should – the Compliance function play in DT and how should the Compliance function future-proof itself to better manage the governance, risk, and compliance (GRC) aspects of their corporation's DT initiatives and better leverage the environment, social, and governance ("ESG") objectives of their company.

To address these questions, the authors interviewed two heads of Compliance at larger multinational corporations and facilitated a Salon hosted by the Digital Legal Exchange, entitled "The Role of Compliance In Digital Transformation: Old Habits Risk Harm". This event was attended by 12 participants including several General Counsel and Compliance professionals. The Salon was conducted under the Chatham House rule. All participants consented to an anonymised write up for these purposes.[4]

The purpose of this piece is to provoke more international, cross border discussion around the role of Compliance in digital transformation.

[1] For a description of Digital Transformation and the role of General counsel and inhouse legal departments (which often have oversight over Compliance departments), see generally Michele DeStefano, Bjarne P. Tellman & Daniel Wu, *Don't Let the Digital Tail Wag the Transformation Dog: A Digital Transformation Roadmap for Corporate Counsel*, 17 J. Bus. & Tech. L. 183 (2022).

[2] Id. at 197-201; id. at 202 (explaining that "[i]n today's corporate environment, legal functions are expected to digitally transform in harmony with the multi-national corporation itself in order to deliver services that are . . . increasingly proactive, client and customer centric, data and metrics driven, tech-enabled, collaborative, and agile, purpose-focused, and where possible, revenue generating").

[3] Shrubs Balsubramanian, *Digital Transformation for the Risk and Compliance Functions*, Deloitte (2018), https://www2.deloitte.com/content/dam/Deloitte/us/Documents/finance/us-digital-transformation-for-the-risk-and-compliance-functions.pdf (last visited April 10, 2023).

[4] A general, anonymized, description of all participants/interviewees' titles and companies is on file with the authors and available upon request.

II. COMPLIANCE´S ROLE IN DIGITAL TRANSFORMATION EFFORTS

A. Baking in Compliance at the start

Unlike Sales, R&D, Supply Chain, Marketing, and other functions, Compliance and Legal are not always included in, or considered critical to, enterprise DT efforts. Instead, work is done in silos and compliance approval is sought late in the game, sometimes too late.[5] Consider the following example:

Let's say the Human Resources ("HR") function wants to launch a new tool to assess employees against a number of different factors to help determine whether their performance merits a promotion or change of role. Traditionally, this is something that HR would design and decide as a function before involving other partners. The HR team may be well-intentioned and their goal is simply to create a fairer and more equitable way to assess employees. However, during the development and planning phase, the HR function may not be considering the legality of using such a tool in all the countries in which the company operates (such as Germany, for example, which is generally very strict) despite the fact that the EU's General Data Protection Regulation ("GDPR")[6] and California's Consumer Privacy Act ("CCPA")[7] regulate how a company collects and handles not only consumers' but also employees' data.[8] In other words, at this point the G in ESG (Environment, Social, and Governance) is not top of mind.

Even if the tool complies with regulations and processes data only for the employment purposes that employees have consented to, the HR team may not be thinking about whether it is "right" or "ethical" to use this kind of tool: Does it accord with the company's stated values relating to the data privacy of employees? Does it align with the company's commitments to the S in ESG, by upholding the social responsibility to protect and respect the privacy of employees', consumers,' partner's, and investors' data whenever that data is collected and processed? Whether the project crosses a threshold legal data protection line or an ethical one, compliance generally isn't involved until after the development phase, at which point they will be asked to assess the project, identify the risks, and suggest remediations. This is true even when the company has a privacy or data ethics officer. By contrast, the IT team is often involved at an early stage, as the team is considered an essential part of the decision-making process whenever a technology solution is purchased or developed. But professionals within companies often do not consider Compliance involvement to be critical to the process, or at least not

[5] Balsubramanian, *supra* note 3, at 2.
[6] *See generally*, General Data Protection Regulation (GDPR), https://gdpr-info.eu/ (last visited April 8, 2023).
[7] *See generally*, California Consumer Privacy Act (CCPA), https://www.oag.ca.gov/privacy/ccpa (updated February 15, 2023) (last visited April 8, 2023).
[8] *See e.g.,* Sara H. Jodka, *The GDPR Covers Employee/HR Data and It's Tricky, Tricky (Tricky) Tricky: What HR Needs to Know, Dickeson Wright*, HRDickensonWright (April 3, 2018), https://hr.dickinson-wright.com/2018/04/03/gdpr-covers-employeehr-data-tricky-tricky-tricky-tricky-hr-needs-know/?utm_source=mondaq&utm_medium=syndication&utm_term=Employment-and-HR&utm_content=articleoriginal&utm_campaign=article; Tully Rinckey, *Responsibilities of Employers under the General Data Protection Regulation*, Lexology =https://www.lexology.com/library/detail.aspx?g=f19963f0-3be2-485c-88d5-dceaece4b446 (last visited April 8, 2023); Peter Todorovski, *Employee Data Processing: What is Right and Wrong Under the GDPR*, PrivacyAffairs (April 7, 2023), https://www.privacyaffairs.com/employee-data-processing/#:~:text=GDPR%20is%20not%20as%20specific%20about%20processing%20employees%E2%80%99,the%20processing%20of%20employees%E2%80%99%20data%2C%20including%20sensitive%20data; *California Consumer Privacy Act: Employee and B2B Exemptions Expire January 1, 2023*, Morgan Lewis (October 14, 2022), https://www.morganlewis.com/pubs/2022/10/california-consumer-privacy-act-employee-and-b2b-exemptions-expire-january-1-2023#:~:text=The%20CCPA%20currently%20imposes%20limited%20obligations%20on%20employers,employees%2C%20job%20applicants%2C%20officers%2C%20directors%2C%20and%20independent%20contractors.

in the "concept phase" of the project. Instead, they recognize that there may be some considerations to take into account, but believe that Compliance and Legal are there to flag them later.[9] Therefore, the development process generally proceeds with HR working with IT to develop or purchase the tech, negotiate with a vendor to on board the solution or collaborate with a development team to design it. Legal or Compliance, on the other hand, are brought into the process late in the day, often raising the legal and/or ethical flags that—as a matter of due course—slow down or sometimes even block the whole project.

This reactive approach (and late involvement of Compliance and/or Legal) is not only due to the attitudes and behaviors of the HR professionals in this example above. Legal and Compliance departments themselves also bear some responsibility for the outcome: often, they do not see their role as being part of the creative and project development process. Instead, they too see themselves as there to uncover a mismatch between a legal or regulatory requirement and what the company is doing – not to propose or build a solution that has a creative element or to be part of a team to create something new. Moreover, there is often not a direct line between compliance and the IT group that develops technology (that could have potential hidden vulnerabilities).[10] Plus, the language involved in some of the technological developments is very complicated and can be challenging for a non-technical person to decode. This invariably results in lots of questions from the lawyers (which at times can be hard to formulate in a way that breaks down the complexity of the topic) that then aggravates the other professionals on the team (especially the IT professionals). On the one hand, this type of questioning by Compliance is understandable because it is extremely hard to green light a project or provide advice or assess the level of the risk without understanding how the tech works and its implications. However, on the other hand, it uncovers the need for Compliance to enhance their technology know-how given how essential it is to do their job effectively and future-proof their value creation for the business teams. To execute their role effectively, Compliance professionals need to be able to map out the technology architecture and associated data flows in order to identify a gap or risk or unintended unethical or biased consequence. They need to do so (to be adept at problem finding) so that they cannot just simply say "no" or overburden the remediation, but actually suggest a creative solution to the problem. In other words, Compliance cannot recommend that the team should implement xyz measures to prevent a certain negative consequence from happening if they don't understand how the tech works, what is the business purpose, and what are the current processes and their impact. To be sustainable and effective, the decision around what measures should be implemented as possible tweaks or fixes should reconcile compliance requirements and the consensus of the teams involved.

[9] Balsubramanian, *supra* note 3, at 2.
[10] Balsubramanian, *supra* note 3, at 2.

B. The rising importance of technological literacy and cross-functional partnership

Compliance professionals who are not technologically literate may become reliant on the IT professionals' interpretation and description of the data flows and technology architecture. The lexicon and focus of an IT professional is of course different from that of a Legal or Compliance professional. This lack of common vocabulary can create misunderstandings between professionals, which can slow down product development and result in negative consequences for the end customer. Consider a simple example like the word "bias". To an IT professional, data is biased by design and certain degrees and nuances are acceptable (if not expected) while others are not and can compromise the data. Either way the word "bias" doesn't have the same negative connotation as it does for a Legal or Compliance professional. Instead, for IT, the word "bias" is rather related to the quality of the data. However, the Compliance professional might provide advice that it is *imperative* that the data has *no* bias. This is completely unrealistic and threatens the Compliance professional's credibility with the IT professionals. So, there is a lack of common language that prevents proper advice and understanding of the scope of the risks. As a result, a stereotypical way of seeing things and proceeding is perpetuated and Legal and Compliance are brought in late in the process, positioned to throw red flags and perceived as blockers instead of professionals that can help problem-find and problem-solve.[11] This leaves Compliance viewed as cops and cost centers instead of strategic business partners[12] whilst uncovering the necessity for this function to overcome traditional, obsolete, frameworks and ways of working that no longer respond to the speed, complexity and uncertainty generated by DT. As one Chief Compliance Officer explained:

> "The function of compliance should be as a business partner which helps us to gain a very high level of trust. People have to understand that we are not the internal police force but business partner consultants who are willing and able to put ourselves in their shoes and try to make their vision into reality. And that's my understanding, that we're a business partner, not a control audit function."[13]

C. New ways of working to address regulatory fragmention

The challenges presented by this way of working are exacerbated by the significant increase in regulation and enforcement in the digital space, the broadening scope of regulation across countries around the world, and the speed at which DT is happening in most organisations.[14] Leading companies

[11] *See* Michele DeStefano, *Chicken or Egg: Diversity and Innovation in the Corporate Legal Marketplace*, 91 Fordham Law Review 1209 (2023) (explaining that lawyers lack the skillsets and mindsets of collaborative innovators and do not spend enough time problem-finding and often have a fixed as opposed to growth mindset which is not conducive to the type of collaboration and innovation corporations need from their legal professionals 1236-1239); Michele DeStefano, *Legal Upheaval: A Guide To Creativity, Collaboration, and Innovation in Law* 44-55 (John Palmer et al. eds., 2018) (explaining why lawyers lack the skillsets and mindsets of innovators and fail to proactively collaborate with empathy, inclusivity ,and an open mind). For more information on the importance of problem finding to innovation see Daniel H. Pink, *To Sell Is Human: The Surprising Truth About Moving Others* 5 (2012); Tina Seelig, *What I Wish I Knew When I Was 20: A Crash Course on Making Your Place in the World 20* (2009) (referring to problem-finding as "need finding"); Tina Seelig, in *Genius: A Crash Course on Creativity* 19–30, 95–102 (2012).

[12] *See* Michele DeStefano, *Creating a Culture of Compliance: Why Departmentalization May Not Be the Answer*, 10 Hastings Bus. L.J. 71 (2014).

[13] Interviewee/Salon Participant #2, Chief Compliance Officer of a Germany-based international pharmaceutical company.

[14] Sanjay Srivastava, *The Blistering Pace of Digital Transformation is Only Going to Get Faster*, Fortune (April 21, 2021, 3:00 P.M), https://fortune.com/2021/04/21/digital-transformation-automation-data-economy-reskilling-retraining/; John de Yonge, *The CEO*

are developing new digital products and services at a dizzying pace.[15] NFTs are a great example. In the past, a company might have years or at least a year to launch something new like an NFT, but now it's in months, in 6 weeks sprints.[16] Another example worth mentioning relates to ChatGPT: the infamous AI tool was adopted by one million users within five days of its release.[17] In contrast, when Marty Cooper, an engineer at Motorola, made the first mobile phone call in 1973, it would take 10 more years before cell phones would be made available to the average consumer.[18] The level of adoption and mainstream access to innovation has never been this fast, triggering new risks and demanding for immediate responses and more preventive approaches.

Given that DT-relevant regulatory frameworks develop quite rapidly to a remarkable maturity level, and the window for implementing regulations is decreasing, complying with increasing local requirements on a local level is one tricky task in itself. Designing and implementing group-wide and global tools that reflect all of the—often contradictory—requirements of the relevant jurisdictions can be highly challenging.

As one Chief Compliance Officer explained,

> "Being compliant when it comes to DT is very hard and that is true for different reasons and the legal complexity of all the legal fields that are linked to DT including data protection. It's pretty hard if not impossible to reach hard compliance because it is happening so quickly, and it is all so new and foreign. So for a multinational corporation, there is an additional level of complexity for being compliant. And it is even more difficult than a cross border check. . . . Multinational companies have to concern themselves not just with GDPR but laws in all the different countries the company has offices in and does business."[19]

A further complication is fragmentation. Different jurisdictions are taking radically different approaches to enforcement. One example is the recent action against Meta, under which Meta was fined €390 Million by the Irish Data Protection Commission ("DPC") after it adopted the finding by the European

Imperative: How Has Adversity Become a Springboard to Growth?, EY (March 8, 2021), https://www.ey.com/en_us/ceo/the-ceo-imperative-how-has-adversity-become-a-springboard-to-growth (reporting that 61% of CEOs "plan to undertake a major new transformation initiative").

[15] Microsoft CEO Satya Nadella claimed that the first two months of the COVID-19 lockdowns forced corporations such as Microsoft to digitally transform more in two months than they had in two years. Jared Spataro, *2 Years of Digital transformation in 2 Months,* MICROSOFT (April 30, 2020), https://www.microsoft.com/en-us/microsoft-365/blog/2020/04/30/2-years-digital-transformation-2-months/.

[16] Simon Blackburn et al., *Digital Strategy In A Time Of Crisis,* McKinsey Digital (April 22, 2020), https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-strategy-in-a-time-of-crisis. Note, research suggests that the pace of technology adoption is faster in the United States than in some other countries. In terms of AI readiness, for instance, a 2019 McKinsey survey found that the U.S. led the world in AI readiness, due to its strong AI ecosystem and positive ICT connectedness. *See also* Jacques Bughin et al., McKinsey Glob. Inst. Notes from the AI Frontier: Tackling Europe's Gap in Digital and AI 2 (2019) (finding that Europe lags behind the U.S. and China in digitization and adoption of AI).

[17] Katharina Buchholz, *ChatGPT Sprints to One Million Users*, Statistica (January 24, 2023), https://www.statista.com/chart/29174/time-to-one-million-users/.

[18] Kevin Lync, *1973: First Mobile Phone Call*, Guinness World Records (August 19, 2015), https://www.guinnessworldrecords.com/news/60at60/2015/8/1973-first-mobile-phone-call-392969.

[19] Interviewee/Salon Participant #2, Chief Compliance Officer of a Germany-based international pharmaceutical company.

Data Protection Board ("EDPB") that Meta's "performance of contract" basis for collecting and processing data for personalized advertising was non-compliant with GDPR.[20] Organizations are being compelled by decisions like these to take accountability for protecting consumers and also for providing more transparency. At the same time, consumers are increasingly aware of their own rights with respect to their data, and less willing to entrust it to third parties.[21] As many participants in the Digital Legal Exchange Salon Event ("DLEX") explained, COVID-19, and the requirements to share data on, for example, vaccination status, heralded a shift in the level of trust that individuals are prepared to place in organizations who are handling their data. As one Chief Compliance Officer explained,

> "It is a jigsaw puzzle of different legal requirements and regulations and my current understanding is that it is impossible to identify and set up and run group-wide processes and tools that actually comply with data protection rules in every level in every country. So we are only talking about harsh compliance and we can pretty much not think about ethics yet."[22]

Plus, there is a gap between what the community thinks is a 'normal' digital life and what the data protection authorities consider lawful. This gap creates a complex tension. Consider that a few weeks ago, the highest data protection authority in Germany ordered the German government to take down its facebook site, and the government refused despite the order. As a result, the Compliance Officer felt compelled to begin internal discussions with his colleagues. He explained to them that

> "this is an absurd situation, that there is a legal requirement on the German government that the government itself is refusing to follow! This begs the question: do we want to and can we use Facebook in our company?"

These are the types of conversations Compliance is having inside their companies because, unfortunately, these kinds of gaps between consumer desires and the legal requirements are a burden to DT in large corporations. It makes it almost inevitable that compliance professionals involved in data protection are seen as slowing things down—because they do, often through no fault of their own. They have to. As this Compliance Officer explained,

> "when it comes to anti-corruption policies, I can apply compliance as a business partner and they accept our recommendations and people like and value what we do for the organization. But when it comes to data protection, where there are a set of rules and regulations that people can't relate to, we have a massive loss of trust as a compliance community. We are considered

[20] Meta Fined €390 Million by Irish DPC for Alleged Breaches of GDPR, Including in Behavioral Advertising Context, The National Law Review (January 20, 2023), https://www.natlawreview.com/article/meta-fined-390-million-irish-dpc-alleged-breaches-gdpr-including-behavioral#:~:text=As%20a%20result%20of%20the%20investigations%2C%20the%20DPC,publishers%20engaged%20in%20behavioral%20advertising%20in%20the%20EU (explaining that the DPC original did not find that Meta was legally noncompliant for relying on the "performance of contract" bases but instead that and that "it did not clearly disclose its purpose for collecting and its usage of the data."); Jennifer Bryant, *Irish DPC Fines Meta 390M Euros Over Legal Basis for Personalized Ads*, IAPP (January 4, 2023), https://iapp.org/news/a/irish-dpc-fines-meta-390m-euros-over-legal-basis-for-personalized-ads/.

[21] According to 2023 the *International Association of Privacy Professional Privacy and Consumer Trust Report*, "[n]early 68% of consumers throughout the world said that they are either somewhat or very concerned about their online privacy. This concern affects how much they trust companies, organizations and governments to collect, hold and use their personal data. Consumers make choices based on their perceptions of privacy, adjusting their compasses in a world awash in data by deleting apps, withholding information and avoiding purchases when they feel their privacy is at risk." Müge Fazlioglu, *International Association of Privacy Professional Privacy and Consumer Trust Report* (March, 2023), https://iapp.org/resources/article/privacy-and-consumer-trust-summary/.

[22] Interviewee/Salon Participant #2, Chief Compliance Officer of a Germany-based international pharmaceutical company.

> the poor guys that are suffering under an unrealistic, unpractical data protection regulation that we are enforcing over them. However, I don't see an alternative approach. As long as we are facing a legal requirement that is way off the people's reality, like the Facebook situation, it is a gap that hardly can be filled. I can't waive my legal reasons even if I understand that it helps the business and is a good DT vision. I can't say let's go for it if it is not compliant."[23]

So, this leads to even more siloed working. If Compliance handles things in a non-practical and non-sustainable way (to the letter of the law that doesn't fit with the company's values, or align with what people at the company or its customers value), data privacy will be perceived as a burden and as a topic with little practical relevance. This could have the unfortunate consequence of relegating Compliance professionals to an enforcement role, rather than viewing them as equal contributors.

Many of the DLEX Salon participants expressed that siloed ways of working are also a threat when it comes to cybersecurity. The cyber threat landscape presents another transformation challenge for Compliance professionals. As the volume of data and the use of technology increases, so does the threat of cyber-attacks and the attention of regulators.[24] The business expects Compliance teams to respond by becoming increasingly mature in assessing and preventing cyber risk. This requires, again, a high level of alignment across business teams, and a high degree of multidisciplinary working. Compliance needs to be right at the heart of these efforts.

True, more and more, executives are recognizing the problem with the siloed, isolated approach and that a more integrated collaboration is needed between the IT, Product Development, Merchandising, Marketing, Legal and Compliance departments. However, as another Compliance Officer explained,

> "very few have figured out how to unblock it and it is unclear how to achieve that given that there is not yet an understanding of what is blockchain, let alone trying to find a more integrated way of working."[25]

This leads to, not only legal risks, but also an ethical slippery slope which can negatively impact the customer. It often falls to the Compliance professionals to consider not just the legal compliance aspects of DT but also how to further the corporation's values and to protect the customer's wants and needs with respect to use of consumer data. This is the focus of the next section of this paper.

[23] Interviewee/Salon Participant #2, Chief Compliance Officer of a Germany-based international pharmaceutical company.
[24] See generally, The Cyber-Threat Landscape: The Digital Rush Left Many Exposed, PWC US Digitatl Trust Insights Snapshot Survey (2021), https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/2021-digital-trust-insights/cyber-threat-landscape.html (last visited April 10, 2023).
[25] Interviewee #1, Global Data Ethics Manager of a multinational beverage and brewing company.

III. UNCONSCIOUS PROBLEM WITH COMPLIANCE´S CURRENT ROLE

A. Operationalizing purposeful innovation and digital ethics

The mission and responsibilities of Compliance are evolving beyond just compliance. Yes, its job is to make sure the company's DT efforts and use of data are aligned with the rules and requirements applicable to the corporation. However, Compliance professionals are not solely responsible for the corporation respecting the law but also for enforcing the company's values (such as DE&I) and ensuring the technology the company is developing can be used to optimize the company's risk management. Furthermore, they are responsible for detecting and addressing the ethical aspects including the real and potential unintended consequences of the projects that a company may launch and also what customers would expect from a trusted organization handling their data.

In our digital world, where product and service choice and convenience offer in the marketplace is at its peak, customers have the option and awareness to give their money and their information to companies that they trust. They are empowered to expect that these companies are living up to their promises to implement a meaningful, purpose-driven, transparent privacy program that includes collection limitations that demonstrate its commitment to its customers' privacy. The opposite, however, is also true. Those companies that don't go further than what is legally required will lose their customers where a competitor is offering more. According to a recent McKinsey report analyzing digital trust, consumers "consider trustworthiness and data protections to be nearly as important as price and delivery time."[26]

Innovation and transformation require flexibility and a "trial and error" approach, which Compliance functions are traditionally adverse to. However, faced with increasingly uncertain and complex scenarios (from both a technological and regulatory perspective), exploring concepts such as user empathy (which is native in Design Thinking methodology) and Agile, can become new tools to address the needs and aspirations of clients and customers.

Importantly, in some ways it appears that the person that is driving the ethical conscience of the company is the Chief Compliance Officer who is doing so almost unconsciously (without the company being conscious of it). And the Chief Compliance Officer is a good fit for this role, in part, because there is so much left unaddressed in the complex overlapping regulations. For example, questions remain around how to group and tag data, about the social and ethical use of group data versus that of an individual, and also how a person is tracked and targeted based on their online activity.[27] Consider for example a cookie banner. There are certain requirements a company has to meet from a data protection standpoint, but nothing prevents a corporation from using certain types of patterns that are known to help nudge customers into accepting vs rejecting a clickable advertisement. Similarly, nothing requires the company to use certain fonts or colors to make something more visually accessible to people with impairments. Today, forward thinking Compliance Officers consider these types of concerns part of their job and critically important to their company's DT efforts.

[26] Jim Boehm, Liz Grennan, Alex Singla, and Kate Smaje, *Why Digital Trust Matters*, McKinsey & Co. (September 12, 2022), https://www.mckinsey.com/capabilities/quantumblack/our-insights/why-digital-trust-truly-matters.

[27] Taylor, L., Floridi, L., & Van der SLoot, B (Eds.) *Group Privacy: New Challenges of Data Technologies* (Vol. 126) (2016); Lillian Edwards, *Data Protection and e-Privacy: From Spam and Cookies to Big Data, Machine Learning and Profiling*, L Edwards Law, Policy, and the Internet (Hart 2018) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3183819.

Given their role in cybersecurity and data protection, Compliance professionals are, of course, involved in updating data protection policies and privacy notices. However, privacy notices are often updated without talking to the customers i.e., to consider what matters to them, and how and when they want these notices, if at all. Currently, reliance is put on opinions, i.e., what consumers SAY they will do if a company is subject to a data breach. Forward thinking Compliance Officers, however, see the act of updating data protection policies and privacy notices, as an opportunity to help their company be more client-centric. Instead of relying on opinions (which can end up validating things that are assumed), they seek user validation by analyzing the data to determine, for example, whether more transparency or more data protection measures really impact behavior. They seek more than simply validating a privacy notice or ensuring that the notice is changed to meet the right glocal rules and regulations, they seek to find out what matters to consumers so that the updates and the overall user experience provide consumer value.

Consider third party advertising. It is a disputed field when it comes to what is allowed legally and ethically. If a person visits website #1, this data can be selected and sold to a completely different third party and the same third party then can use it for their own ads. Forward thinking Compliance Officers at progressive companies who are dedicated to ensuring their customers trust the way they use their data (and believe it will make a difference in purchasing behavior by customers) are trying to go one step further than simply ensuring legal compliance. They are thinking deeply and strategically about the issues related to third party advertising and whether the selling of that data to third parties is ethical and in line with the values of the company. They are also considering whether such advertising has the right type of messaging and transparency around it, so as to not breach the company's commitment and consumer's expectations.[28] Similarly, forward thinking Compliance Officers are having discussions with Marketers within the company who can track users' activity to provide a personalized, customized experience which, on the one hand, might delight the customer. As such, privacy and data protection can be a force for good, in improving the user experience, particularly when the focus is on using only the data that is needed and processing it in a way that consumers can reasonably expect and appreciate. However, on the other hand, even if the company has taken the right steps before collecting the information,[29] using it in this way, it might make them worried about their privacy and scare them away. In the era of surveillance capitalism,[30] if a company suddenly puts an ad up in front of a customer of one of its products that might relate to their activity, it might put people off. In fact, sometimes it even raises concerns for people because they do not understand how the data stream is working. They may even think their computers or phones are being watched, listened to or tapped by the company that has now put the advertisement in front of them which can create people to distrust a company and walk away. However, as one Compliance Officer explained,

> "the common denominator across regulation in the digital space is transparency. Not only do organizations need to be compliant, they also need to be able to explain their approach and

[28] To Personalize or Hyper-Personalize? The Paradox of Privacy and Targeted Advertising, Ardent Privacy Blog, https://www.ardentprivacy.ai/blog/to-personalize-or-hyper-personalize-the-paradox-of-privacy-and-targeted-advertising/ (last visited April 8, 2023).

[29] Id. ("Online marketers also need to be aware of how data privacy laws regulate their practice. Laws such as the EU's GDPR, California's Consumer Protection Act (CCPA), California Privacy Rights Act (CPRA), and Virginia's Consumer Data Protection Act (CDPA) currently regulate the collection and sharing of data, which requires companies and marketers to take certain steps before collecting information and using it for marketing purposes.").

[30] John Laidler, *High Tech is Waiting for You: Q&A with Shoshana Zuboff*, Harvard Gazette (March 4, 2019), https://news.harvard.edu/gazette/story/2019/03/harvard-professor-says-surveillance-capitalism-is-undermining-democracy/.

actively to demonstrate compliance. In this way, regulation demands an ethical response, not simply a response that is compliant."[31]

B. The rising implications of ESG

Similarly, ESG frameworks are changing, to take into account the tensions between cybersecurity, digital ethics and privacy—which are new and emerging elements in the ESG reporting space.[32] This reporting obligation presents its own challenge: how can the value of data ethics and the safeguarding of privacy be measured? What metrics can be used to validate success? How can companies measure and communicate cultural change and new ways of working? Data Ethics and Compliance professionals will be challenged to define the metrics that can evidence the value they bring to the business. But as all the participants in the DLEX Salon event agreed: Evidencing a return on the internal investment required for digital ethics is challenging. However, as the unconscious conscience of the company, it is the Compliance Officer's job, in collaboration with other functions, to start to develop the metrics to measure and determine if there is a business case for ethical compliance that is in line with the corporation's values and promises (and that goes above and beyond the letter of the law).

IV. CONCLUSIONS AND A FEW RECOMMENDATIONS

That Compliance Officers are taking on this role is laudable and sensible. As others have remarked, they have the motivation and ability to be the conscious of the company, to ensure that considerations beyond the letter of the law (ethics, and consumer desires and preferences) are taken into account from the beginning during the problem—and opportunity—finding stages and all the way through all phases of product development and launch. Yet, the current siloed ways of working have consequences that make it almost impossible for the Compliance Officer to do a good job of being that unconscious conscience. This is due to a few factors.

First, like the other department heads, Compliance Officers also often have limited access to data, they are focused on their individual department mandates, and they cannot always look at risk signal data holistically and go beyond what is legal to what is ethical.[33] As such, as others have pointed out, sometimes Compliance only has access to "a limited data set that is directly related to compliance. . . [T]hese data silos often keep risk teams from seeing the complete picture."[34] As the Chief Ethics & Compliance Officer at a multinational technology company shared, "One challenge is access to data and gaining support from the IT function."[35] The participant's organization "has grown through acquisition, and data integration has been complex. They are working to apply AI to enable proactive fraud analytics across the business; however, progress is hampered by access to the IT function, as compliance as a function is not IT's highest priority."[36] Although agreeing, the Global General Counsel for

[31] Interviewee #1, Global Data Ethics Manager of a multinational beverage and brewing company.
[32] See BlackStone, ESG Policy, https://www.blackstone.com/wp-content/uploads/sites/2/2022/02/BX-Firmwide-ESG-Policy.pdf) (last visited April 7, 2023).
[33] Sean Thompson, *Why the Next Era in Risk Management and Compliance Requires Digital Transformation*, Forbes (November 9, 2022), https://www.forbes.com/sites/forbesbusinesscouncil/2022/11/09/why-the-next-era-in-risk-management-and-compliance-requires-digital-transformation/?sh=7c4af0c7e351.
[34] *Id.*
[35] Salon Participant #12, VP, Chief Ethics & Compliance Officer at a Fortune 500, multinational technology company.
[36] *Id.*

a global engineering company explained the catch 22 that some are facing "a tension between the requirement on organizations to demonstrate transparency and accountability and an increased trend towards data localization. It is challenging to digitally transform if data is 'locked down' and not accessible to mine for insight."[37] In other words, the right governance ensures that processes and policies are in place to help digital efforts scale and make them accessible across different teams and jurisdictions, but data is a critical enabler. It is the key to helping uncover common pain points, to validate trends, and to ensure consistency across different business lines and jurisdictions.

Second, the siloed way of working prevents cross-functional teams that understand each other's ways of working and also prevents a consistent approach across jurisdictions which is critical. Organizations need a unified standard to allow them to measure and compare levels of risk. This requires a high degree of alignment across the business, and a high level of consensus. Only with that, will teams have accountability i.e., clarity as to who has accountability for processes and outcomes.

Third, with the existing silos and negative consequences mentioned above, it is near impossible to demonstrate value. Evidencing a return on the internal investment required for digital ethics is challenging. It is akin to a cultural transformation, having a long lead time before it will bear fruit. Building a business case based on this intangible value is impossible with the current siloed approach. Similarly, measuring objectives and achievements for digital ethics and ESG in the context of compliance is a challenge.

As one of the participants of the DLEX Salon aptly explained,

> "in order for the Compliance Officer to move beyond being seen in traditional 'policing' role and be able to use the data and technology to transform the business, and develop a coherent business case in support of the change, the Compliance Officer needs the authority to create proofs of concept; and, more than that, it needs senior sponsorship, and a high level of collaboration with the support by other teams in the business to work together to effect large scale, transformational change."[38]

Only then, will Chief Compliance Officers be able to spearhead projects that provide the company insights that allows them to map risks based on the type of asset and the nature of the risk and identify gaps that need to be addressed, leverage data to find patterns and areas that require intervention to prevent anti-corruption, and most importantly, help operationalize ethical and customer-centric principles across the business, making the abstract principles concrete so that everyone is working to not only comply with the law but also to meet and exceed expectations of clients.

Lastly, the ultimate goal is that the role of the Compliance Officer, that may be currently an unconscious conscience of the company, be out in the open and, more than that, embedded in all functions of the company. It is imperative that the departments across companies do not solely rely on Compliance to catch or fix the ethical issues but to design projects that embed the ethical conscience when handling the data to create that value for consumers. As a Senior Corporate Legal Counsel of a global bank who participated in the DLEX Salon, explained,

[37] Salon Participant #9, Global General Counsel of a Fortune 500, multinational corporation engineering, electrification, and automation company.
[38] Id.

> "Digital transformation is the responsibility of the entire enterprise. Marrying compliance with digital transformation is particularly challenging. It cannot be reduced to individual KPIs. instead, each individual has to take accountability for a compliant transformation, with all employees being taught how to manage risk in an ethical way."[39]

As noted earlier, this essay is merely a thought-piece, based on a limited amount of research and a lot of qualitative and anecdotal evidence. That said, our purpose is aspirational and so we conclude on an aspirational note with a quote by one of the Chief Compliance Officers we talked to:

> "Being compliant is the base element of being ethical but there is so much more. That's why being a Compliance professional right now might be the best job in the world especially if you are a Lawyer Compliance professional because then you are not the person only reviewing the provisions of a contract. Instead, you get to help people fulfill a future position in a safe and ethical way and that is very motivating and drives me."[40]

[39] Salon Participant #5, Senior Corporate Legal Counsel of a multinational financial services company.
[40] Interviewee/Salon Participant #2, Chief Compliance Officer of a Germany-based international pharmaceutical company.