Consistency and transparency: Getting connected products to reflect organizational values

By Breann McNeil, MJ, CCEP-I

Breann McNeil (mcneil_breann@elanco.com) is Senior Advisor, Anti-Corruption and Third Party Management, for Elanco Animal Health in Greenfield, Indiana, USA.

- linkedin.com/in/breann-mcneil

From tennis rackets to crockpots, "smart" products are now available everywhere for the general consumer. On a daily basis, companies are considering how consumers might want to use technology in everyday items, what will control the devices, what services will be attached to use the device, and how they would interact on the Internet of Things (IoT). If the organization you are working for does not yet have a connected device or service related to IoT in the marketplace, it is only a matter of time.

Ethics and compliance (E&C) has an important opportunity—and responsibility—during this digital shift. Most of us are familiar with compliance risks in these connected devices and IoT, typically focused on privacy or cybersecurity. But thinking in a silo when evaluating your organization's exposure in this area is no longer effective.

The ethics and compliance officer can choose to embrace the coming changes, actively learn about the products and their role in the company's strategic future, or they can avoid it because they don't understand the space. Avoiding it guarantees that E&C will miss key conversations that could protect both the company and the future stakes of the IoT network and the design of related devices.

Crossing over industry lines

There is a huge global network being created that brings together Big Tech as well as organizations previously in separate, independent industries. The network comes without true collaboration focused on appropriate self-regulation of an evolving industry.

Manufacturers of cars, appliances, pet products, and other items are experienced in meeting the safety and quality requirements of their specific industries. However, they are unprepared to meet these same requirements once they enable a product to be recognized and controlled by an IoT-related device. These companies are now exposed to a digital industry they've never previously been a part of and are connecting with partners originally thought to be completely unrelated.

Product development reflects internal values

To know how the IoT industry will fare if E&C does not encourage internal development and exercising of principles, all we need to do is look to examples, such as healthcare and entertainment ratings, which have demonstrated the consequences of failing to comply with reasonable, organizational-level, internal principles to establish widely accepted industry self-governance.

In each of these areas, consumers are met with myriad conflicting local, national, and international regulatory

requirements that make it near impossible for them to make informed purchasing decisions by using like comparisons across various jurisdictions. Because there are limited physical boundaries on the use of IoT, ethics and compliance professionals must do themselves a favor and get involved proactively to address the complexities of regulatory enforcement.

Low organizational standards set low industry-level standards, which drive low consumer expectancy standards. This downward spiral leads to poor application of smart, connected, or artificial intelligence-enabled devices and incomplete, inaccurate data fed to the overarching IoT. A quick search of the internet will lead to a number of articles demonstrating how this spiral is already happening and must be corrected before competing regulations make future product design and marketing a compliance nightmare. Connected consumer product development requires immediate consideration of internal organizational values and principles driven by cross-functional input.

Basic framework of internal principles

No two companies will have identical IoT development principles. Product lines and risk appetites will be different; this is not a copy and paste exercise. However, there should be some similarities in the framework to build a foundation toward successful self-regulation and governance on an industrywide level.

Accountability to the industry and other manufacturers/developers

The most difficult areas for an industry to monitor to maintain credibility include (i) identifying unethical performers to sanction them appropriately, (ii) conflicts of interest, and (iii) competent performance. Once an organization has been in an industry for some time, especially within a geographic region, they will notice the constant exchange of talent between major workplaces. Some former employees will also leave to form new businesses. Unless an employee leaves the industry (willingly or unwillingly), the ties and familiarity of this group will, intentionally or unintentionally, shield peers who are not performing to proper standards. Many consumer product manufacturers have realized that the actions of a small number of unethical or incompetent performers can put a mark on the entire industry and, if the negligence is severe enough, invoke consumer demands for regulatory actions that can forever alter the course of IoT and their businesses.

Physicians have long emphasized that the complexity, skill level, and knowledge base required to even understand the subject matter involved makes it too difficult for nonmedical experts to apply healthcare regulations. Similarly, unless the IoT industry begins to self-regulate openly and forcefully, and communicate that bad actors (individuals or organizations) will not be tolerated, both the industry and society will lose when regulators ultimately take action to completely overhaul the governance structure.

Just as your organization would not want to be known as substandard for product quality, it should not be willing to settle for substandard quality in the IoT network. Examples of next steps to take include:

- Working cross functionally to bring cyber, privacy, legal, quality, and ethics into the development and data use conversations. Keep a seat at the table by staying curious.

- Creating a strong business plan on why the company needs to take a position on this. Lack of participation now will only result in stifled product development due to regulatory enforcement in the future.

- If you have a leadership development group, encouraging them to get the executive team to take a field trip to visit a company they'd like to replicate.

Transparency with consumers

When a consumer purchases a product or service enabled to interact on IoT, they do not comprehend the deep scope of the number of players involved. The industry, therefore, has a duty to enhance transparency and participation to set up a global governance scheme for success.

Additionally, consumers have repeatedly demanded transparency until they feel they are being heard. For example, physicians convinced society that "science-based medicine was superior to alternative therapies and that their profession represented a trustworthy moral enterprise."[1] Over the years, however, the industry has failed to provide transparency in billing, diagnosis, and treatment options.

Another example is of a survey conducted by the Federal Trade Commission. The responses indicated that parents wanted and welcomed help in identifying which entertainment products might not be suitable for their children.[2] Parents desired transparent information so they could make informed decisions.

Start providing transparency to your consumers by:

- Using a focus group to study your external website, review product package information, or call customer service. Where do they feel confused or misled?

- Working closely with privacy and cybersecurity personnel. They are already putting in some efforts on transparency. Make sure it is a cross-functional effort.

- Thinking like a parent, because many consumers are. They expect to have trust and transparency in a product to perform in the manner presented to keep both themselves and their child(ren) protected.

Consistency

Consistency in product information is required to set reasonable expectations of performance, even if the outcome is not known. Self-imposed consistency is necessary because domestic legal systems often fail to provide a level solution. The result has been that whenever one local government regulates sales and distribution channels and marketing methods, companies will simply choose to operate from another. Manipulation of local laws occurs easily with intangible objects like data collected from an IoT device.

Consider the gap found in the entertainment rating industry. The structures and scopes of the rating/labeling systems are different for each entertainment industry (video games, music, and films); these systems are used to advise parents about violent content unsuitable for children, and they may discourage to different degrees the marketing or sale of violent products to minors. The issue in this example, which generally occurs with IoT product security and application, is the lack of consistency that leaves a confused, uninformed consumer not knowing what they are purchasing. As fluid as the functionality and data collection already is with IoT, the public cannot afford to have inconsistency.

Consistency could be achieved by considering:

- What standard labeling levels already exist in the product category?[3] Are they applied clearly to products to assist consumers in considering IoT implications when reading packaging?

- Networking with others within the same product industry. Proactively propose what could be improved across all products within the same category to increase consistency.

- Requiring your company to put minimum ethical standards for development in their playbook. Do not allow new product approval without the standards being met.

Oversight and enforcement

In the entertainment ratings industry in the US, films are assigned a rating based on a review from an independent panel. The panel participants must have parenting experience and no connection to the film industry. However, the approval of selected panel participants happens by the president of the Motion Picture Association of America.[4] A majority vote from the panel sets a rating for a feature. An appeal of the rating can occur from the producing company and goes through an appeal committee made up of members of the industry. This committee often allows the appeal for lower rating than the original film rating the parental panel assigned, thus submitting a younger audience to desensitization. Seemingly, the independence of the process has been lost.

Eventually, a September 2000 Federal Trade Commission report to the president on the lack of industry self-regulation standards in the entertainment ratings system required all three entertainment industries (TV, movies, and video games) to increase accountability immediately by (1) establishing or expanding codes of conduct, (2) imposing sanctions for violations, (3) increasing compliance at the retail level, and (4) increasing parental understanding of the ratings and labels.

Transparency, consistency, and ethics must come together to help boost consumer confidence. Why must an industry wait for regulatory enforcement before action is taken? IoT product developers across the globe agree that the more regulation there is on product design, the harder it will be to create innovative products. But the IoT industry, with the help of their ethics and compliance colleagues, must first demonstrate they can effectively monitor and enforce ethical design and create more consumer trust.

Effective internal governance could include:

- Autonomy of security or application ratings panels that would be kept sacred and demonstrate to regulators and consumers that these values are unwavering.

- Using enforcement examples, such as the one described above, to develop key controls for the governance of development.

Get tech savvy

E&C can no longer avoid becoming more technologically advanced. We must immediately challenge ourselves to be more involved, to encourage ethical design, and to help drive the regulatory developments in the space. Your organization already has some sort of digital strategy. Make sure ethics is a part of it before compliance has to step in.

Takeaways

- Try thinking like a consumer as you work on internal principles with your organization, not just as a corporate risk manager.

- Set a professional development goal to understand your company's portfolio of smart consumer products —sit in a sales onboarding or business development meeting.

- Communicate with leadership regularly on ethical or regulatory developments that could affect connected product development or key partnership arrangements.

- Reach out to connected or smart consumer products chief compliance officers. Encourage and challenge each other to think outside our typical compliance evaluation processes.

- Don't be complacent. Speak up if you see that ethical design or use of data could be a potential issue in new product development.

1 Sylvia R. Cruess and Richard L. Cruess, "The Medical Profession and Self-Regulation: A Current Challenge," *Virtual Mentor* 7, no. 4 (April 2005), 320–324, https://bit.ly/2T7Idcp.

2 Federal Trade Commission, *Marketing Violent Entertainment to Children: A Review of Self-Regulation and Industry Practices in the Motion Picture, Music Recording and Electronic Game Industries*, September 2000, https://bit.ly/3iWX1F1.

3 Shane D. Johnson, John M. Blythe, Matthew Manning, and Gabriel T.W. Wong, "The impact of IoT security labelling on consumer product choice and willingness to pay," *PLoS One* 15, no. 1 (January 2020), https://bit.ly/3nPlorS.

4 Federal Trade Commission, *Marketing Violent Entertainment to Children,* 53–55.

Become a Member Login