12 RESPONSIBLE TECHNOLOGY: ADVANCING TRUST AND SECURING THE ECOSYSTEM

Ajay Bhalla

Responsible technology—new and emerging technologies like AI, biometrics, and cyber—stand to perform an unprecedented and positive role for society. But for them to be successful, public, government, and industry trust is essential.

How, then, can an environment be created and sustained that strikes the right balance between enabling technology development to continue to keep pace with user demand, while ensuring the right guardrails are in place so that we can all build and maintain trust in them?

12.1 WHERE WE ARE

12.1.1 It's about Trust

My friend was talking about driverless cars recently. "If my car crashed as often as my computer does—I'd be worried," she said. "And if my computer was *driving* my car, I'd be terrified."

Of course, those who design driverless cars are only too aware of the leap of faith required for people to trust their lives to a machine. That's why they invest so much in research, testing, and security. The technology needs to be infallible. It needs to be *trusted*. The only way my friend and millions of others will get into a car that drives itself is when they trust the technology behind the wheel.

Trust can be defined as "a confident relationship with the unknown."[1] Engendering that confidence is the big challenge facing innovators today. Your new technology may be great, but will it be *trusted*? Gaining this trust is becoming more important because people are being asked to entrust much more of their lives to technology. My friend will tolerate her computer crashing every now and then if she only uses it for Netflix, Twitter, and her daily news feed. She won't tolerate a computer crashing her car, messing up her home security, and sharing details of her private life with the rest of the world.

12.1.2 Challenges

When we look around, there are plenty of examples to undermine our confidence in new technology. We're familiar with the little horror stories: the talking toy doll that can be hacked by anyone with a smartphone,[2] the fish tank connected to Wi-Fi that lets fraudsters access a Las Vegas casino database,[3] and the virtual voice assistant that emailed an individual's private conversation to a work colleague.[4]

And there are the big horror stories: the Equifax hack in which the personal data of half the population of the United States was stolen;[5] the Cambridge Analytica scandal, which still reverberates around Facebook; and the cyberattacks on power stations in Ukraine and against oil pipelines in Turkey.

12.1.3 Digital Convergence and the Internet of Things

There are a number of reasons for this insecurity, not least the fact that the internet evolved to connect people, not to make them feel secure. This connection didn't matter so much when our online lives were separate from our offline lives. It *does* matter now that they are intertwined. Whether it's your phone connected to your watch, home, or car, everybody has multiple interconnected devices—we're never really offline. It is anticipated that by 2025, 50 billion devices will be connected to the internet,[6] each of them a link in an enormous chain. Some strong, some weak, some smart, some dumb. The casino was hacked through a thermometer, the pipeline was hacked through a video camera, and the doll was hacked through a $2 microphone. Cheap, insecure, and often peripheral devices can become ticking time bombs on the internet of things.

12.1.4 Exponential Growth in Data

These connected devices are creating an exponential growth in data; 90 percent of it has occurred in the past few years alone.[7] New technologies like 5G will further accelerate this growth. But while we may *create* the data, we often don't own it, control it, know who has it, or who will use it. In theory we should know, but when was the last time you actually read a clickwrap agreement? A group of university professors once calculated that it would take seventy-six working days to read all the privacy documents one agrees to in a single year.[8] Even if our data starts off in a secure environment, there's no guarantee it will stay there.

12.1.5 Age of Artificial Intelligence

There's an important reason that data is so sought after—it is the fuel for artificial intelligence (AI). AI is wonderful. It is being used to improve crop yields, tackle world hunger, predict earthquakes, and transform health care. But we need to ensure that the insatiable demand for data doesn't undermine our digital ecosystem in the way that the race for oil and gas has created problems for our natural ecosystem.

These are *the principal challenges that face innovators today. It's no longer acceptable to just "move fast and break things," to place innovation and product development above all else, not least security and well-being.*

12.2 A GUIDE TO RESPONSIBLE INNOVATION

So what should we be doing instead to foster responsible innovation? It starts with security by design. In the following pages I will outline a high-level guide to responsible innovation.

12.2.1 Security by Design

First, recognize that every connected entity needs to be a secure entity, no matter how small or apparently insignificant. If it can't be secured, it shouldn't be connected.

Second, responsibility for security lies with the producer, not the end user. Millions of connected devices haven't had a security update in years, because the owner hasn't done so. If it can't be patched remotely, it shouldn't be connected.

Third, secure the network. Even a safe car becomes unsafe on dangerous roads. In the real world, this safety is a collective endeavor: dedicated planners design and build the highway network, automobile manufacturers make sure their vehicles are safe, police ensure that users abide by the rules, and governments and industry bodies regulate all of the above. It's time we gave our superhighways the same consideration.

At Mastercard we know something about security by design. We are custodians of a network that processes 75 billion transactions per year. That means securing not just every card, payment device, and terminal on the network, but also the payment rails that connect them. There's good reason for putting security at the heart of this. Financial institutions are three hundred times more likely than businesses in other industries to suffer an attack.[9] For banks, cybersecurity is now their top board-level priority;[10] they're investing heavily to stay ahead of the criminals. Industry bodies like our own—EMVCo—have for many years set standards and specifications in payment security globally.

12.2.2 Privacy by Design

The second tenet of responsible innovation is privacy by design.

For too long, personal data has been considered a commodity rather than a possession. Privacy by design challenges this notion. It means minimal data collection—only what is needed, not what is wanted. It means giving individuals control of their data and how it is used, rather than having them sign it away in clickwrap contracts. And it means handling their data with the highest standards of security and integrity.

Privacy by design is at the heart of Mastercard's new ID service. The company is creating a user-centric digital identity that is owned, managed, and controlled by the individual and requires neither further aggregation of identity data nor the creation of centralized data structures.[11]

This doesn't stop Mastercard from innovating to harness the societal value of data. Anonymized consumer transaction data has limitless applications for development research, for example. By allowing researchers to use data-driven insights, the Mastercard Center for Inclusive Growth is assisting in new programs to improve the economic growth and financial inclusion of the world's vulnerable communities.

12.2.3 Use Security to Drive the Consumer Experience

Third, align security with the consumer experience. This is crucial. Do not trade security for convenience.

Take the example of biometric authentication, where the password is replaced with the person. Techniques like fingerprint and facial recognition are far more secure than knowledge-based solutions, such as passwords, PINs, and logins. Think of the hundreds of accounts, passwords, PINs, and memorable data you've accumulated. It's no surprise that most people choose passwords that are easy to remember and then use them across multiple accounts. This practice makes individuals vulnerable to fraudsters. Biometrics provides a solution by enabling the automated recognition of individuals according to physiological traits—fingerprint, face, or voice, for example. Explicit biometrics such as fingerprint, face, or palm can be combined with passive biometrics (behavior) and device ownership to enable multifactor authentication and frictionless transactions.

The main driver for biometric adoption is not security but the fact that 90 percent of users prefer the experience.[12] It's why Mastercard put usability at the heart of its Five Factor Framework to help financial institutions adopt biometrics.

12.2.4 Ethics and Governance

Finally, a word on the role of ethics and governance in technology innovation.

Technology can be used for good or bad. AI, for example, has implications for security and privacy. It can be deliberately misused by bad actors. Unwittingly, it can also introduce bias and discrimination in decision-making and propagate or amplify biases inherent in the data. In commerce, the self-reinforcing nature of AI products can create monopolies and encourage herd behavior. Machines may be capable of complex calculation, but so far they have been unable to make qualitative or moral judgments. So the next time a company tells you it's using AI to take care of business, ask who's taking care of the AI. And if the whole thing sounds like a black box, walk away, for the sake of all of us.

Mastercard has committed to an AI governance framework around the core values of trust, integrity, and respect. It follows a process that begins with an evaluation of the intended purpose for which we want to use AI, then moves through data and model evaluation, design and risk scoring, and continued monitoring for bias and unintended consequences. The organization has established similar principles for the use of privacy and data too.

This isn't just about obeying the law. For one thing, legislators can't keep pace with technological innovation. The General Data Protection Regulation (GDPR), for example, is a success story that took years to debate and implement. For all its strengths around the protection of consumer data, it now finds itself at loggerheads with one of the most transformative technologies of the modern era—blockchain. GDPR mandates the "right to be forgotten," but distributed ledgers are designed to last forever. They are decentralized and immutable—a tamper-proof record that sits outside the control of any one body. GDPR isn't disappearing, and neither is blockchain. But the industry, both businesses and regulators alike, needs to work closer together to build an environment where new technologies like blockchain can thrive and evolve, while still ensuring that the right accountability safeguards are built into the way they are developed. There are other challenges with open banking, where new players are entering a sector whose security is challenged more than any other. Open banking rules force financial institutions to share data, whereas GDPR rules restrict them from doing so.[13] One regulation rubbing up against another.

There is no simple answer to this, except to say that doing things right requires thought, cooperation, collaboration, and mutual support. In our digital ecosystem we are codependent as never before. It is possible to succeed responsibly; Mastercard created a seamless and secure payment network that operates across hundreds of countries, thousands of stakeholders, and billions of transactions. We have long understood that securing our network means securing our customers, merchants, cardholders, and the wider ecosystem too.

12.3 RESPONSIBLE INNOVATION AND TRUST

Responsible innovation creates trust, and trust keeps the world turning.

I do believe that one day my friend will allow herself to be driven by an autonomous vehicle. The time will come when she takes a leap of faith and steps inside, but not before she's confident she'll be safe. People are often being asked to take a leap of faith these days—trusting technology they don't understand, giving data to people they can't see, forming relationships with businesses they don't know.

And no matter how impressive the innovation or how dazzling the technology behind it, the decision of whether to trust it will be made by the smartest machine that exists—the human being.

NOTES

[1] R. Botsman, *Who Can You Trust?* (London: Portfolio Penguin, 2017).

[2] "#Toyfail: An Analysis of Consumer and Privacy Issues in Three Internet-Connected Toys," Forbrukerrådet, December 2016, https://www.forbrukerradet.no/wp-content/uploads/2016/12/toyfail-report-desember2016.pdf.

[3] A. Schiffer, "How a Fish Tank Helped Hack a Casino," *Washington Post*, July 21, 2017.

[4] S. Wolfson, "Amazon's Alexa Recorded Private Conversation and Sent It to Random Contact," *The Guardian*, May 24, 2018.

[5] T. S. Bernard, T. Hsu, N. Perlroth, and R. Lieber, "Equifax Says Cyberattack May Have Affected 143 Million in the U.S.," *New York Times*, September 7, 2017; S. Cowley, "2.5 Million More People Potentially Exposed in Equifax Breach," *New York Times*, October 2, 2017.

[6] Some forecasts, such as from International Data Corporation, show up to 75 billion devices by 2025, but we say over 50 billion to be conservative (e.g., "Connected Devices Will Generate 79 Zettabytes of Data by 2025," *IoT Business News*, August 10, 2020, https://iotbusinessnews.com/2020/08/10/08984-connected-devices-will-generate-79-zettabytes-of-data-by-2025/).

[7] M. Belfiore, "How 10 Industries Are Using Big Data to Win Big," *Watson Blog*, July 28, 2016, https://www.ibm.com/blogs/watson/2016/07/10-industries-using-big-data-win-big/.

[8] A. M. McDonald and L. F. Cranor, "The Cost of Reading Privacy Policies," *I/S: A Journal of Law and Policy for the Information Society* 4, no. 3 (2008): 543–568.

[9] R. Ungario, "Cyberattacks Are 300 Times as Likely to Hit Financial Firms Than Other Companies: A Sweeping New Report Finds

They're Not Prepared," *Business Insider*, June 20, 2019, https://markets.businessinsider.com/news/stocks/cyberattacks-impact-major-threats-to-financial-firms-not-prepared-2019-6.

10. J. Boehm, P. Merrath, T. Poppensieker, R. Riemenschnitter, and T. Stahl, "Cyber Risk Measurement and the Holistic Cybersecurity Approach," McKinsey & Company, November 18, 2018, https://www.mckinsey.com/business-functions/risk/our-insights/cyber-risk-measurement-and-the-holistic-cybersecurity-approach.

11. Mastercard, https://www.mastercard.us/en-us/issuers/products-and-solutions/mastercard-digital-identity-service.html, accessed July 12, 2021.

12. G. Lovisotto, R. Malik, I. Sluganovic, M. Roeschlin, P. Trueman, and I. Martinovic, "Mobile Biometrics in Financial Services: A Five Factor Framework," conference proceedings, July 11, 2017, https://newsroom.mastercard.com/eu/files/2017/06/Mobile-Biometrics-in-Financial-Services_A-Five-Factor-Framework-compressed3.pdf.

13. D. Bonderud, "Open Banking and the Closed Ecosystem: The Tech Banks Need to Navigate GDPR," *BizTech*, September 23, 2019, https://biztechmagazine.com/article/2019/09/open-banking-and-closed-ecosystem-tech-banks-need-navigate-gdpr#:~:text=Security-,Open%20Banking%20and%20the%20Closed%20Ecosystem%3A%20The,Banks%20Need%20to%20Navigate%20GDPR&text=To%20meet%20the%20growing%20demands,application%20program%20interfaces%2C%20or%20APIs.