TECHNOLOGY LAW ASSOCIATION NEWSLETTER

INTRODUCTION

Welcome to the inaugural edition of the Technology Law Association's (TLA) newsletter. The TLA was founded in the fall term of 2020 by Chelsea Angel with the vision to explore the role of a lawyer working with clients in the technology sector who require legal expertise from a business, entrepreneurial and finance perspective. In that spirit, these newsletters are meant to draw attention to exciting developments at the intersection of law and technology and to serve as a resource for students considering pursuing a career in the technology law space.

As technology evolves to acquire an ever more intimate and ubiquitous presence in our lives, technology law has emerged as a unique subset of legal practice. Boutique firms like Oziel Law and Wires Law have emerged to address the demand head-on while a number of full-service firms including Stikeman Elliot, Osler and McCarthy Tétrault staff dedicated teams of technology law specialists. Though curiosity and necessity attracts us to cases where technology exposes an issue for which existing legal doctrines provide no remedy, technology law draws upon familiar legal traditions in ways which even the Luddites among us would be familiar. Some of these practice areas include trademark and in--tellectual property protection, contracts and licensing, start-up and business formation, mergers and acquisitions, securities and capital markets, domestic and international information privacy and data protection and cybersecurity law.

TABLE OF CONTENTS

More than others, the subject matter of technology law can be awash in hype and buzzwords. Combined with the trite observation of law lagging behind innovation, one might be excused for having an anachronistic impression of the law or for doubting its ability to respond to emerging challenges. The prevalence of this view, that technology is uniquely 'unregulable', has roots in libertarian, crypto-anarchist and cypherpunk philosophy and has been seized by many progenitors of our modern technological infrastructure. However, to what extent is it the case that technology is uniquely 'unregulable' rather than it being the case that creators of 'disruptive' technologies have deployed these philosophical schools of thought to create this impression because shooing away regulators makes good business sense? Prompted by election interference, the Cambridge Analytica scandal and the mounting anti-trust battle (among others), the 'unregulability' of tech line of argument is losing force as government intervention ramps up and the era of 'move fast and break things' breaks down. As the saga between the law and technology evolves, it will be the continuing responsibility of the legal community to safeguard our democracy, privacy, autonomy, security and prosperity from threats posed to thereto by unchecked innovation. In this newsletter we learn about Bill C-11 and the proposal to modernize Canada's private sector privacy legislation, blockchain and the securities regulation of cryptocurrencies, legal and operational challenges surrounding smart contracts and artificial intelligence ethics.

Semester At A Glance

On November 19, 2020, the TLA hosted an interesting and successful panel discussion on technology law and emerging technologies including blockchain, artificial intelligence and fintech. We were joined by Sam Ip and Zain Hemani who work in technology law at Osler, Niloofar Entizari who works in capital markets at Blake's and by Christine La Fleur who is corporate counsel at Salesforce. Sam and Christine were quick to remedy the common fear and misconception that in order to practice in technology law one must come from an engineering, computer or natural science background. That said, Niloofar stressed how vital it is for her to develop a conversant understanding of her clients' business – technology included. Having graduated from Western Law in 2019, Zain noted how commercial and intellectual property law courses offered by practicing lawyers have been most instrumental in his practice at Osler.

Bill C-11 Seeks Privacy Law Overhaul

BY MICHAEL GORA

Bill C-11 seeks to enact the *Consumer Privacy Protection Act* (*CPPA*)[1] while repealing corresponding provisions from the *Personal Information and Protection of Electronic Documents Act* (*PIPEDA*). Heralded as long overdue by many privacy advocates and critics of *PIPEDA*, the *CPPA* represents Canada's effort to modernize privacy legislation in the wake of the European Union's *General Data Protection Regulation* and the American's *Californian Consumer Privacy Act*. Tabled on November 17, 2020 by the Minister of Innovation, Science and Industry, Navdeep Bains, the *CPPA* is currently at first reading and is likely to change as it makes its way through the legislative process. That said, understanding how the *CPPA* stands to impact the technology sector is crucial as businesses large and small begin to ask questions about how to recalibrate their privacy practices to stay ahead of the changes. Indeed, the European and Californian experiences suggest that an organization's pro-active compliance with the *CPPA* will be scrutinized during investors' or prospective buyers' due diligence inquires.

While many of the fair information principles found in *PIPEDA* would carry over to the *CPPA*, the *CPPA* would modify the scope of some and add others to the list. For example, while consent would remain at the heart of the regime, the *CPPA* would carve out service provider and business operations exemptions to the general consent requirement and it would add that consent must not be obtained through deceptive practices.[2] Individuals can also request that an organization dispose of personal information held about them subject to legal retention obligations or where it can't be severed from others' personal information.[3] In blockchain applications, where immutability is baked into the technology, the right of an individual to request their personal information be disposed of could pose technical and legal challenges.

Added to the list would be rights to data portability,

---

[1] *Bill* C-11, *An Act to enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to make consequential and related amendments to other Acts*, 2nd Sess, 43rd Parl, 2020 [*CPPA*].

[2] *Ibid*, ss 16, 18, 19.

[3] *Ibid*, s 55.

de-identification and algorithmic transparency. Data portability would provide individuals with the right to request that an organization transfer the personal information it has collected about them to another organization.[4] The impacts of data portability are most eagerly awaited in the fin-tech space given the Federal government's involvement in open-banking discussions. The proposed rules around de-identification seek to restrain how even de-identified data can be used,[5] potentially expanding the law's jurisdiction beyond personal information. As Michael Geist notes, the public battle over the Sidewalk Labs project in Toronto illustrates that some people object to the use of their de-identified information. Finally, where an automated decision-making system is used to make a prediction, recommendation or decision about the individual, the organization must, on request by the individual, provide him or her with an explanation of the prediction, recommendation or decision and of how the personal information that was used to make the prediction, recommendation or decision was obtained.[6] The utility of this right will depend on the extent to which an organization can flout its obligations by either appealing to the need to protect its proprietary information or the inherent unintelligibility of its 'black box' algorithmic system.

Motivating compliance with the new and improved privacy protections by the *CPPA* would be the dollar figures associated with their breach. Whereas *PIPEDA* might have been criticized for lacking teeth, the *CPPA* would be a shark. The *CPPA* would create a Personal Information and Data Protection Tribunal which would be charged with reviewing decisions of the Office of the Privacy Commissioner (OPC) and could impose administrative monetary penalties of up to $10 million or 3% of an organization's gross global annual revenue for contravention of processing provisions and certain security safeguard provisions.[7] For more serious offences, such as where an organization knowingly contravenes the *CPPA* by obstructing an OPC proceeding, an organization could face a criminal conviction and face a fine of up to 5% of annual global revenue or $25 million, whichever is greater.[8] These penalties would be the harshest of their kind in all of the G7. The *CPPA* also provides individuals with a private right of action against organizations in contravention of the act.[9] Associates at Tory's suggest that businesses might see increased litigation activity here because proving loss suffered by an organization's breach of a statutorily imposed duty may provide litigants with a clearer pathway to recovering damages than through existing common law causes of action including privacy torts, negligence or breach of contract.

For businesses, the potential for penalties, fines and liabilities generated by the *CPPA* may significantly increase risk portfolios and questions remain about whether these costs can be insured or indemnified. For privacy advocates and beneficiaries of the proposed regime the *CPPA* would provide a sorely needed update to a privacy regime eclipsed by technological change. On top of the business and consumer interests in the *CPPA* are Canada's broader strategic priorities. For one,

---

[4] *Ibid*, s 72.
[5] *Ibid*, ss 74-75.
[6] *Ibid*, s 63(3).
[7] *Ibid*, s 94(4).
[8] *Ibid*, s 125(a).
[9] *Ibid*, s 106.

prolonged legislative stagnation in the area of privacy law generates the risk that Canada could lose its adequacy designation *vis a vis* the *GDPR* which would impact cross border data flows between Canada and the European Union. Second, lurking in the background of these legal and regulatory debates is the Canadian government's desire to ground domestic and international technological development in a rights-based framework. In this light, the *CPPA* would signal how Canada is willing to walk the walk as much as it's willing to talk the talk. In competition with this objective is the goal of promoting Canada as fertile ground for technological innovation through programs like the Pan Canadian AI-Strategy which have contributed to economic growth in the information communications and technology sector (ICT) which has vastly outpaced other industries.

Blockchain: Exploring The Regulation Of An Unregulated Technology

BY CHRISTINE PHILLIPS

Whether it is from an enthusiastic cousin over family dinner or from Season two of Mr. Robot, you've likely heard of blockchain in one form or another. The techspeak surrounding blockchain can be intimidating enough to prevent further research (examples include words such as hashing, nonce, and Merkle Root). That said, it is possible for non-computer scientists to wrap their heads around the conceptual framework of blockchain. For future lawyers, a baseline understanding of how the technology operates may prove to be critical.

Blockchain is the technology that underpins the majority of crypto-assets, such as Bitcoin. The technology was first introduced in 2008 in Bitcoin's whitepaper published by the infamous Satoshi Nakamoto (an individual or group of individuals whose identity remains unknown).[1]

Maybe you're asking yourself why we should even bother learning about blockchain. Although it may seem like an esoteric technology reserved for computer science grads and crypto day-traders, blockchain has been referred to as the next internet. For one thing, Bitcoin has been trading at record highs. BTC traded comfortably between $50,000 and $60,000 throughout February 2021 in what some referred to as "Crypto-Mania". This was shortly after reaching a record high of $20,000 in December 2020. But blockchain is by no means limited to Bitcoin. Developments in applications such as smart contracts (discussed in the next article), title registries and personal identity data management are just a few examples of how blockchain is disrupting tech as we know it. As this wave continues, it will bring myriad legal questions and challenges along with it. But first things first – what is blockchain?

I have found it best to understand what blockchain is by first understanding what it is not. Efficient marketplaces require trust and a mechanism to prevent double-spending (that is, a buyer that pays for something without having the funds to do so). Traditionally, the source of this trust is a central authority such as the central bank as well as intermediaries such as your own personal bank. These authorities verify each transaction in order to assure payees that the transaction is valid and legitimate.

Bitcoin seeks to achieve this same level of trust without the need for an intermediary using block-

[1] Satoshi Nakamoto *Bitcoin: A Peer-to-Peer Electronic Cash System* (March 2009), online: Bitcoin < https://bitcoin.org/bitcoin.pdf.

chain. Transactions are broadcasted and collected by a distributed network of "miners" who compete to bring these transactions into a block using a complex calculation.[2] These blocks in turn are copied to a ledger which is then replicated and maintained for all participants of the blockchain. The result is a permanent, immutable, incorruptible record. Payees can therefore verify a transaction as legitimate without the need of a traditional financial institution; in this regime, trust is sourced from consensus in the network.

Blockchain is regularly associated with cryptocurrency, or more specifically, with Bitcoin. This is nothing more than a proprietary eponym (similar to how we call tissues "Kleenex"). However, it is important to understand that there is more to blockchain than Bitcoin or cryptocurrencies.

The focus of this article will be on the application of blockchain to crypto-assets and the resulting legal questions that arise therefrom. The distinctive nature of crypto-assets will touch several domains of the law including criminal, estate planning, bankruptcy, contracts, consumer protection, tax and privacy/security. In this article, I will touch only on the efforts to regulate trading cypto-assets.

LEGAL IMPLICATIONS OF CRYPTO-ASSETS

How can a regulatory body stake governance over an asset that is inherently unregulated? In the absence of a central authority, regulation has fallen mostly to crypto dealers and exchanges. This raises many questions, chief among them, how are crypto-assets legally defined?

WHO AM I?

Similar to me after my fourth midterm exam, crypto-assets are facing something of an identity crisis. They fail to fit neatly within the definitions of currency, commodity or security. This lack of specific categorization will have profound implications in terms of regulatory and tax treatment of crypto-assets.

Bitcoin for example, can be used as a means of barter and sale and represents a unit of value, thus satisfying the traditional definition of currency.

Bitcoin also has certain indicia of a security. Purchasers will buy and hold their coins out of an expectation that these will appreciate in value over time in a manner similar to trading equities. What is more, start-ups and innovative projects have taken to fundraising via Initial Coin Offerings ("ICOs")[3] where tokens are traded in exchange for dollars or other cryptocurrencies. These tokens offer rights to future profits not unlike an Initial Public Offering (IPO).

Crypto-assets also share attributes with commodities, which are defined as a basic good in commerce that can be exchanged with goods of the same type (think gold, natural gas and oil). Bitcoin, along with other crypto-assets, falls within this definition. Investors can choose to exchange cryptocurrency using assets of its same kind or choose to buy derivatives such as futures contracts, similar to how one may trade commodities.

---

[2] Nakomoto, *supra* note 1 at 3.

[3] Filippo Annunziata, "Speak, if you can: what are you? An Alternative Approach to the Qualification of Tokens and Initial Coin Offerings" in Bocconi Legal Studies Research Paper Series (Milan: Bocconi University Department of Law, 2019). https://dx.doi.org/10.2139/ssrn.3332485.

All this to say that the precise categorization of crypto-assets is far from settled, posing a unique challenge for regulators. Luckily for us, this means lots of work for lawyers.

THE STORY IN CANADA (SO FAR)

The Supreme Court of Canada laid out the four-prong test to establish whether or not something is a security in *Pacific Coast Coin Exchange of Canada v Ontario (Securities Commission)*.[4] The *Pacific Coast* test asks:

1. Whether there was an investment of money;
2. In a common enterprise;
3. Involved an expectation of profit;
4. Which was solely from the efforts of others.

This test was utilized by the Canadian Securities Administrators (CSA) in the first official publication regarding the application of securities legislation to crypto-assets and ICOs: CSA Staff Notice 46-307 Cryptocurrency Offerings. The publication outlined the CSA's framework to determine whether applicable securities legislation will apply, including evaluating the nature of the transaction, as well as any relevant policy considerations, in conjunction with the *Pacific Coast* test.

The result was that in many instances, tokens and coins sold in ICOs were characterized as securities. The notice continued to confirm that any cryptocurrency exchanges (online exchanges that facilitate purchase and sale of cryptocurrencies) offering coins/tokens characterized as "securities" were bound to abide by the relevant securities legislation. In Canada, capital markets are provincially regulated. Ontario's securities law is administered by the Ontario Securities Commission (OSC) which administers the Ontario *Securities Act* and other securities legislation.[5]

Compliance with securities legislation can be a challenge for crypto-assets. For one thing, it has become standard practice for coins and tokens to issue white papers preceding the launch of a coin.[6] The white papers provide general information about the coin or token as well as the underlying blockchain technology. To date, there are no uniform regulations governing how these white papers should be structured.[7]

In contrast, under the Ontario *Securities Act*, a person or company cannot trade a security in absence of a preliminary prospectus filed with the OSC.[8] White papers fall short of these prospectus requirements.

CSA REGULATORY SANDBOX

The CSA is not one to stifle financial innovation so thankfully, crypto exchanges are not stopped dead at securities legislation. Recognizing the challenges encountered by crypto dealers and exchanges, the CSA offered the Regulatory Sandbox, an initiative to "support fintech businesses seeking to offer innovative products, services and applications in Canada." The sandbox offers temporary exemptive relief from applicable securities legislation. In Ontario, this falls under the OSC LaunchPad team.

To date, there have been several successful

---

[4] [1978] 2 SCR 112 [*Pacific Coast*].

[5] RSO 1990, c S 5.

[6] Annunziata, *supra* note 4 at 12.

[7] Annunziata, *supra* note 4 at 12.

[8] RSO 1990, c S 5, s 53.

applications under the CSA Sandbox.[9] However, it is not clear what this means for the future of crypto-asset trading in Canada.

WHAT'S NEXT?

This is surely not the last time we will hear of blockchain (I'm looking at you, future lawyers). The race between the law and technology has hardly ever been close and blockchain came to win. The challenges and questions that arise as our law accommodates this issue will be some of the most interesting to follow throughout our careers. And with that, Canada's story with blockchain is just getting started.

A Primer On Smart Contracts

BY MICHAEL GORA

In 1997, legal scholar and cryptographic pioneer Nick Szabo defined a smart contract as a computerized transaction protocol that executes the terms of a contract. Despite frequently being associated with blockchain, the idea of the smart contract predates blockchain and virtual currencies. Many, if not all of us, would be familiar with the predecessor to the modern smart contract, the vending machine - it takes in coins, and via a simple mechanism, dispenses change and a product according to the displayed price. Modernly, smart contracts run on blockchain technology by companies like Ethereum that employ computer programs designed by contracting parties to execute an agreement provided that a series of if/then conditions are met.

There are two ways to think about how a smart contract can be put to use. In the internal model, the code forms the entire legal agreement between the parties, superseding any document written in natural language. In the external model, a smart contract is only used to enforce certain terms of a contract otherwise written in natural language. In both cases, smart contracts are best suited to applications where measures of performance are highly objective. For example, AXA is a French insurer that uses smart contract technology to provide immediate compensation to a flight passenger whose flight is delayed more than two hours. Because smart contracts utilize blockchain's trust enhancing and cryptographically secure technology, they may also be able to reduce the costs traditionally associated with intermediaries. As such, will and estates law, real estate law and escrow arrangements have been flagged as sectors of the economy most suited to the adoption of smart contract technology.

A smart contract is potentially a misnomer in two ways. First, they are categorically distinct from other smart technologies like a smartwatch or smart phone which leverage data mining and artificial intelligence in their operation. That said, it is through the expansion of smart technologies and the internet of things into new environments that will drive the growth of smart contracts by gathering data and increasing the scope of actionable and objectively verifiable inputs. The construction industry is particularly interested in the marriage between internet of things and smart contracts by programmatically linking payment to the satisfaction of predefined indicia such as delivery of goods, hours logged or weather conditions.

---

[9] *Impax Finance Inc (Re)*, 2017 LNONOSC 490; *AngelList LLC (Re)*, 2018 LNONOSC 299; *ZED Network Inc (Re)*, 2019 LNONOSC 240; *Wealthsimple Digital Assets Inc. (Re)*, 2020 LNONOSC 314.

It is worth noting how smart contracts' reliance on third-party data providers sits in tension with their claim to reduce reliance on intermediaries and thereby increase security and eliminate points of error. These third-party sources called 'oracles' are necessary to provide input about some external state of the world such as snow accumulation or time of delivery in order for the smart contract to execute or not execute a term of the agreement.[1] Blockchain developers who create these oracles or allow third-party data to interface with smart contract blockchain providers like Ethereum receive a small cryptocurrency payment in exchange for the use of their oracle. It is possible that these oracle providers will come to play central roles in the execution of smart contracts. Depending on how this sector of the smart contract economy develops, choosing one preferred oracle over another to facilitate the execution of an agreement may be a hotly contested term negotiated by contracting parties.

The second way a smart contract might potentially be a misnomer pertains to whether one can be a contract at all. This question has yet to come before a Canadian court. For the most part, the unique nature of a smart contract shouldn't strain a court's analysis of the requisite elements of a contract - consensus, consideration, intent, capacity and legality. However, potentially unique to smart contracts is whether a contract expressed purely in computer code to the exclusion of all natural language generates the level of certainty required to be legally enforceable. Related is the question of whether a purely codified contract would satisfy the *Statute of Frauds* requirement that some contracts be in writing. As alluded to above, the more common use cases for smart contracts are where parties seek to programatically execute certain terms of a contract otherwise natural language contract. In these cases, the binding agreement could serve as an objective indication of the parties intentions. This 'external model', related to the idea of the Ricardian contract, which keeps one foot in the natural language world and the other in the codified world would appear to provide contracting parties with the greatest degree of certainty for the time being.

Finally, because smart contracts programatically compel performance of obligations, courts will not need to enforce them by ordering damages or specific performance. The greater challenge will arise where a party seeks to undo a smart contract that was entered into via fraud, misrepresentation or mistake but can't because of the immutable nature of blockchain.[2] Here, courts will be called upon to undo void or voidable smart contracts after they have been executed using tools like recession and restitution using monetary payments as substitutes for the aggrieved party's loss of crypto currency (such as Bitcoin or Ether) or other assets.[3]

Aneeq Hashmi On Artificial Intelligence, An Interview

BY CHELSEA ANGEL AND GOLSA HASHEMI

Golsa and I [Chelsea] had the distinct pleasure of

---

[1] Florian Martin-Bariteau & Marco Pontello, Hashing out Agreements: An Overview of "Smart" Contracts Under Canadian Law (June, 2020) online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3592986.

[2] Though immutability isn't strictly absolute and there are ways to edit or reverse entries to a blockchain, Andrew Luesley notes how these solutions are "only helpful where parties are using trusted smart contracts or are programming them themselves." Andrew Luesley, "Unravelling Smart Contracts: Smart Contracts and the Law of Rescission in Canada" (2019) 19 Asper Rev Int'l Bus & Trade L 155 at 173.

[3] *Ibid* at 155-56.

interviewing Aneeq Hashmi, a Senior Director at PWC Consulting, to glean his insights on artificial intelligence and its impact on society. Aneeq is one of the greatest technical minds I have ever met. We met while working in the world of technology consulting. I can vividly recall the time in the lunchroom when Aneeq expertly explained the difference between artificial intelligence and intelligent automation to me. Aneeq is distinguished not only by his professional achievements, but also his strength of character. He is guided by a keen sense of ethics and morality that permeates everything he does. When the idea arose to write an article on artificial intelligence, I knew I could rely on him. He has always been there for me, whether I needed reference letters or general advice.

Without further ado, here is the transcript from our interview:

Question 1 - Could you tell us about your background and expertise in technology?

Answer: My name is Aneeq Hashmi. I am the Senior Director for Artificial Intelligence and Applied Analytics within the Salesforce consulting division at PWC. Using machine learning, AI, dashboards, and predictions, I fine tune them to surface insights that are meaningful for different personas within our client organization. All the data that we've gathered on people are to build on three things: 1) the current relationship status with the customer, 2) the context of that relationship, and 3) how to provide that directional indicator to the future of that relationship to improve your bottom line. By giving the right insights, we allow customers to make better decisions providing an overall better customer experience.

In terms of my background, I'm not a traditional technologist. I followed what I wanted to do and what I wanted to learn, and I'm still doing that. However, I find that intrinsic satisfaction at the end of the day, outweighs the money that I make. One of my hopes is that there are still people like me out there.

I started out in Pakistan. Then I came here to the University of Ottawa to study Computer Systems Engineering. I decided to transition from the telecom industry into software development. After working at Accenture, I joined PWC, a private partnership company where the rules are more personal relationship based involving more value-based determination and judgment.

Question 2 – If you had to describe artificial intelligence to someone with no technical background, what would you say?

Answer: McCarthy and Minsky, the forefathers of AI, described it as anything that a machine can do that was done previously by a human. That was an archaic definition since now there's several different tasks that machines can do that classify as automation and not intelligence.

One of my favorite definitions these days is the way Google describes AI rather as the machines' ability to adapt and improvise in a new environment and to generalize the knowledge that it has and apply it to brand new unfamiliar scenarios. Intelligence is not a scale or attribute itself. It's how well and how efficiently you can learn that quantifies that intelligence.

To expand upon that, there's two kinds of prevailing AI today; narrow AI and general AI. Narrow AI are specific tasks, like I developed an artificial intelligence software that helps me book cheap flight tickets. But I can't ask this AI software to then tell me the fastest route to the air-port. In narrow AI, the developed abilities and

skills are specific to a limited degree of tasks. On the other hand, general AI is AI that's about as efficient as an actual human being, as the computational progress of a human brain and can do anything and can learn anything. Sort of like a human assistant where you can ask it to do anything and it will try because its applicability is to internal purposes.

Question 3: What do you have to say to people who fear AI and its capabilities?

Answer: In my opinion, people have to dial back from the science fiction. The threat posed by artificial intelligence and robots really isn't that they're going to become evil and kill us all. They're going to cause a rapid increase in the wealth, inequality and economic disparity that exists today to such an extreme that the quality of life for the majority of human beings will quite literally become untenable. It's a political problem. It's a regulatory problem and it's a society problem that needs to be solved. It demands a serious political solution.

Mass automation alone poses that challenge because the more you automate, the less people you have working. So, you need things like universal basic income, legislation, taxation. But from a legal perspective, artificial intelligence carries the capability to make autonomous decisions without human input. However, I must say that where we are today is quite far from that inflection point where people need to be worried. The challenge to date with AI is the same as any other new technology; it's a regulatory and political social challenge.

Question 4: Where do you see the future of ethics in AI?

Answer: Drawing on Dr.Thilo Hagendorff's paper on AI ethics, he mentions that there are guidelines and principles that have been developed for how technology developers should adhere to ethics. The question then is do these guidelines actually impact or change human decision when it comes to developments in AI? In short, the answer is no. The reason is that ethics in general lacks the ability to enforce its claim as there isn't really a clear delineation between an ethical guideline and its enforcement. Part of the challenge is that there's a lot of different viewpoints on which ethical guidelines should be adopted and what's considered to be "ethical" in general. Can ethical guidelines really be effective?

I believe that there is a way and that is for ethicists and technical people to interact effectively. As of now there exists a gap between the two groups and the solution is to bridge that gap. Ethicists are unwilling to learn technical knowledge while technical people don't work to learn from ethical considerations as they don't see the real-world applications of them. The scientific discipline must stop themselves from trying to control or limit ethical guidelines. Classical ethical approaches aren't going to work. You're going to have to augment them by applying some kind of value or virtue-based ethics to aim at value directed development so that ethics aren't just going to be a checkbox but rather a tool for advancement. As technical contributors, we must expand the scope of where ethical guidelines apply and uncover the blind spots that exist. Lastly, ethicists should be embedding themselves within technology groups to learn a day in the life of technology and better understand the practical challenges of this field.