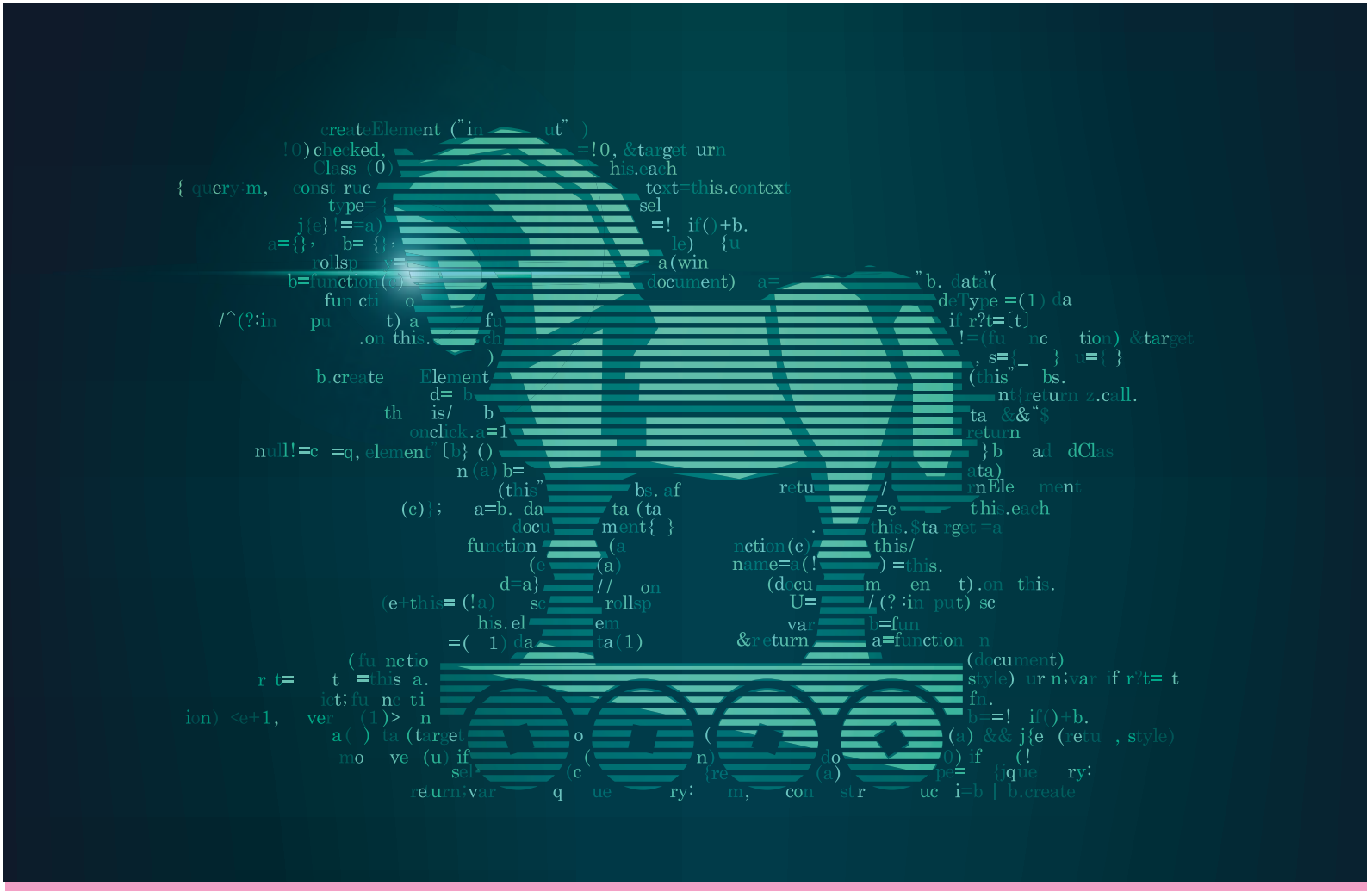

PRIVACY IN A TECHNOLOGICAL AGE

BY
SUSAN JOSEPH

Executive Director of Cornell FinTech Initiative, Cornell University, SC Johnson College of Business, CEO/CoFounder Health-Trends.AI, CEO, SusanJosephLLC- JD/MBA blockchain consulting, Executive Director, Diversity in Blockchain (nfp).

TechREG CHRONICLE
MAY 2022

Visit **www.competitionpolicyinternational.com** for access to these articles and more!

PRIVACY IN A TECHNOLOGICAL AGE
By Susan Joseph

In our data-driven society, privacy as a fundamental right should be recognized and upheld. We must adopt strong legal and technological protections that preserve our autonomy. Legally speaking we must establish a comprehensive federal scheme that recognizes privacy as a fundamental right. Technologically speaking, solutions that are architecturally developed from the individual privacy point of view should be deployed. These trust frameworks will need to mesh with new laws that support privacy as a fundamental right. New types of decentralized/blockchain identity systems are coming online and evolving which support privacy rights and restore the balance of power between the individual and service provider. These systems are disruptive, potentially very profitable, and will impact status quo business models. Tensions between the old and new will have to be resolved. With legal and technological means working together, we can protect our right to be left alone. Privacy is possible in the digital age.

01

INTRODUCTION: PRIVACY RIGHTS IN OUR DATA-DRIVEN ECONOMY

What does privacy as a fundamental right mean? How does that right fare in a data-driven society? How can we protect privacy through both legal and technological measures? Answers to these questions will define how we will be able to live our lives as they are increasingly intertwined with, and influenced by, existing and emerging technologies.

02

WHAT DOES PRIVACY AS A FUNDAMENTAL RIGHT MEAN?

The right to privacy is one of the foundational precepts on which our stated constitutionally protected rights rely. Our right to autonomy and dignity is presupposed by the First (right to be an independent person), Fourth (right to be secure) and Fifth Amendments (right to refuse to self-incriminate). However, our Constitution does not explicitly enumerate a right to privacy.

In 1890, soon-to-be Supreme Court Justice, Louis Brandeis famously defined the right to privacy in a Harvard Law Review article as "a right to be left alone." Our technologically connected world did not exist back then, but the law certainly contemplates the protection of the person which extends to and covers his digital self as a representation of his personhood. In a digitally intermeshed world, are we able to be both connected and left alone? This question, and Justice Brandeis' definition take on new importance as privacy is continuously under attack in today's data-driven world.

Laws must evolve in response to technologies and societal changes. For instance, copyright law was created long ago in response to the introduction of the then revolutionary technology, the printing press. Today's digitally connected world requires a federal explicitly enumerated right of privacy to carry out the Declaration of Independence's fundamental assertions that we have an inalienable "right to life, liberty, and the pursuit of happiness." Congress and industry have taken note, and there are privacy bills under consideration. It is time to envision a comprehensive baseline federal law that imposes a strong duty of care with both remedial and significant penalties and consequences together with a Digital Bill of Rights.

03

OUR DIGITAL STORIES ARE SHARED BUSINESS

A. What Data is Collected?

It is often said that the collective "we" is the product, in this age of "surveillance capitalism." Every aspect of our lives can be captured and exploited for commercial gain by tech companies and others through collected data — data that should be protected under federal privacy laws. Some examples of data routinely collected by private businesses include our face prints, iris scans, location, purchase habits, sleeping habits, photos, voice recordings, fingerprints, the way we drive, how we exercise, what we read, what information we search for, who we know, how we use appliances and lights within our homes, etc. This information can be stored indefinitely, retrieved immediately, sold to many, and used to devise targeted marketing and profiling.

B. How is Our Personal Data Generated and Who Collects It?

Data is generated through a variety of online and mobile activities. A 2020 estimate calculates that 2.5 quintillion bytes (number with 18 zeros) of data are generated daily. This dizzying pace gets more impressive, when you consider that the bulk of the data generated in the world has occurred in the past two years. This data consists of both Personally Identifiable Information ("PII") which is defined as information that can be used to identify us and the broader spectrum of personal data, defined as information generally about us.

A sampling of the latest 2022 statistics show that in an internet minute, 231 million emails are sent, 5.9 million Google searches occur, 694 million songs are streamed, 16.2 million texts are sent and 2.1 million are active on Facebook (Meta). Much of our personal data is generated through internet searching. Google dominates the search arena by conducting ninety-five percent of all mobile searches and 90 percent of all desktop searches in the U.S.

Other companies also routinely collect and use our data to fuel applications and target us. Facebook is one such avid data collector

and marketer. A leaked document from Facebook as reported in The Guardian states that Facebook collects trillions of data points daily. It is thought that the company tracks and collects 52,000 data points on every user observing us in many cases even after we leave the platform.

Data generated and collected through sensors in devices from appliances to cars to buildings is on the rise. Despite chip shortages and other supply chain disruptions in 2022, the number of connected devices (Internet of Things) is expected to grow to 14.4 billion and reach 27 billion by 2025. The amount of data coming online is almost incomprehensible.

Let's look at the seemingly straightforward example of smart light bulbs. Did you know that Amazon and Google collect data from these "smart home" implementations? They increasingly require that a light bulb controlled by a smart speaker continuously provide status reports to its hub. And the information acts as a tracker to our daily lives. As a recent insurance journal article succinctly puts it: "Even light fixtures, in elaborate setups, are a map of home life: When do you get home? When does the light in your child's bedroom usually go off? What days do you burn the midnight oil?"

Or, look at the connected doorbells that have made their way into our lives. Ring's terms of service state that you grant them an unlimited, irrevocable and perpetual license to use the content which may include audio, images, video, or text. You may not want to consent to this automatic and passive method of collecting your data; and you may not even be aware of it.

04

YOUR HOME MAY BE YOUR CASTLE, BUT YOU HAVE ALLOWED IN A TROJAN HORSE OF ADVANCED HOME TECHNOLOGY AND SMART DEVICE PROVIDERS

A. What do Companies do with Our Data?

Companies make predictions from our data to select and nudge our behavior toward product and service purchases or to influence our relationships, associations, and voting choices. We are regularly micro and macro targeted. The applications that we use seem to fit us so well because they are created from and for us. And, they offer a carefully cultivated window to influence and shape our future. Some companies, like Facebook, feed millions of data points into algorithms which offer up six behavior predictions per second that can be marketed and deployed to advertisers who seek to influence our interactions. Facebook's approach is particularly powerful as it directs relatively personalized targeting to connected individuals subject to social influence.

The dark side of this bargain is that a David and Goliath style power imbalance favors very large technology service providers over consumers who have little choice to decline the surveillance and targeting because alternative products and services are not otherwise widely available. The "consent" to terms of service more similarly resembles a contract of adhesion than a level playing field. An individual is bound by thousands of words of obscurely written privacy policies and one-sided terms of service that he would have to weed through to determine if/how he could even take protective action. The reality, of course, is that almost no one has the time or expertise to read and understand these policies.

There have been some strong public repercussions for companies both collecting data and sending it to third parties to review. Tech companies now provide consumers with directions to turn off much of the data collection in many instances, but that is not a comprehensive or complete solution. And turning off the tracking options may not effectively protect your privacy. Google is currently being sued about its data gathering practices by the attorneys general of the District of Columbia, Texas, Washington, and Indiana who claim the company deceived consumers who revoked access to location data by continually surveilling them to obtain the data. When you consider that Google basically commands the data search market, the alleged overreach of data collection is staggering.

The end result is that our personal data is circulated and used both individually and in aggregate well beyond what we thought we permissioned, and we have custodied it with BigTech or other companies without adequate assurance of its safety and downstream transmission.

B. How Big of a Problem is Data Oversharing?

Many are familiar with Facebook's (now Meta) Cambridge Analytica and the misuse of our data that affected global elections. In that example, our dignity and very autonomy, not to mention our government, civil stability and well-being were targeted and manipulated. And just recently, The Wall Street Journal reported that Google, through its Project Nightingale, is collecting millions of medical data records from Ascension without patient or doctor consent to analyze for health care insights and patient care suggestions. That program has triggered a federal investigation.

Technology companies did not start out to control our every move. And we did not start out expecting to be controlled. Amazon, Google, and Facebook, for instance, sprouted a mere generation ago and brought technological innovation to the world with the goals of connection, information access, and convenience. Unfortunately, along the way, they morphed their business models. The online advertising industry grew with them, evolved, and largely eviscerated our privacy while they were looking, but we were not. It is time for us to seriously start looking.

05

COMPANIES HAVE NOT HONORED OUR TRUST

At the end of the day, we have to ask, at what cost is all of this convenience? We have come to expect that our data will be mishandled. Companies seem to have lost the ability to be good data stewards. The list of data breaches continues to grow. Once trust is broken, it is hard for a company to reclaim it. Several of the more egregious breaches from 2021, 2022, and recent years are listed below.

· **Misconfigurations of cloud services?** Names, email addresses, dates of birth, chat messages, location, gender, passwords, photos, payment information, phone numbers, and push notifications of more than 100 million Android users exposed.

· **Leaked database?** Emails and phone numbers of Facebook users from 106 countries, including more than 32 million records of U.S. users exposed.

· **Server breach?** Cash App (owned by Block) 8 million customers contacted about a hack of customer names, stock trading information, account numbers, portfolio values, and other sensitive financial information.

· **Plain text data storage risk?** See Equifax where an estimated 147mm people were affected and a recent FTC settlement of up to $700 million penalty was assessed.

· **Fingerprints and facial recognition potentially compromised?** See Suprema, which exposed 28 million records of over 1 million people worldwide.

06

LEGAL FRAMEWORKS CAN BE CREATED THAT PROTECT OUR PRIVACY

A. Strengthen the Right to Privacy

The Supreme Court in Griswold v. Connecticut in 1965 explicitly stated that guarantees in the Bill of Rights have penumbras which create zones of privacy. In other words, the right to privacy exists, is recognized, and protected — at least within certain bounds. Over the years, the implied right to privacy in the Constitution has been further expounded upon by the courts and legislatures. Specific statutory rights to privacy have also developed which limit access to PII such as HIPAA and others. However, no comprehensive federal law yet exists that creates a well-regulated and orderly scheme to protect our data and our privacy.

Our data is multifaceted. It has property-like characteristics. It is also an information flow that we necessarily must share in certain instances and keep to ourselves in other situations. Consider who actually owns my photo data when I share it with a social media site such as Facebook.

From an information flow perspective, suppose I post a group photo that includes me and other non-Facebook members. Is the photo owned by all, and must we all consent to its posting and posting afterlife? What if one of us wants to take down that photo posting? How does a non-Facebook member know the photo is posted or even ask for it to be deleted? Can I require that Facebook delete all information related to that photo posting including comments by others? What about the re-posts that have occurred? Does anyone have the right to take them down?

From a property rights perspective, if Facebook wants to monetize the use of my information, should I have the ability to be compensated? How are non-Facebook members who have not permissioned the use of their data compensated when their information is shared? What are the original poster's data ownership rights including compensation regarding the downstream sharing of posted information to third parties?

Simply treating data as property devalues the way data is used and respected in society. It is problematic to think of data as simply another piece of property. As a recent Brookings article states:

> "Treating personal information as property to be licensed or sold may induce people to trade away their privacy rights for very little value while injecting enormous friction into free flow of information. The better way to strengthen privacy is to ensure that individual privacy interests are respected as personal information flows to desirable uses, not to reduce personal data to a commodity."

07

CALL TO ADOPT A CONSTITUTIONALLY PROTECTED DIGITAL BILL OF RIGHTS

The most fundamental privacy protection is envisioned as a constitutionally protected right. A natural outflow of that protection is a Digital Bill of Rights clearly setting forth the rights and responsibilities of those who handle data.

An MIT Technology Review article outlined some general principles for a Data Bill of Rights. Those rights include:

· The right of the people to be secure against unreasonable surveillance shall not be violated.

· No person shall have his or her behavior surreptitiously manipulated.

· No person shall be unfairly discriminated against on the basis of data.

Federal law can draw from other legal frameworks that protect privacy. California has enacted privacy laws. Other states have enacted laws. However, a patchwork of state privacy laws that affect digital transmissions across state lines can very quickly become messy, hard to navigate, provide uneven protections, and be difficult to enforce. A more consistent approach would be to create strong federal protections.

Other governments have implemented proactive and protective privacy laws. The General Data Protection Regulation ("GDPR") enacted by the European Union is a good step toward accountability for companies who collect and use our personal data. It provides significant financial consequences for violators as well as remedial actions to protect individuals. It attempts to restore the balance of power from an asymmetric relationship to one that is fairer. These advancements sound encouraging. In addition to legal protection, technological solutions can help champion this right.

08

TECHNOLOGICAL SOLUTIONS CAN BE IMPLEMENTED THAT PROTECT PRIVACY

A. Data Minimization Principals Should be Followed

The principal of data minimization, collecting and retaining only that data that is necessary for the stated purpose, can be applied to protect privacy and identity. Since identity determines how you are counted and can transact, let's look at the components of digital identity.

B. Components of Digital Identity

· **Claims**: an identity claim is a statement made by the individual. One that contains two claims could be: 'My name is Mary, and my date of birth is June 28, 1979." This can also be thought of as an attestation.

· **Verifiable Credentials:** Documentation that provides evidence for the claim. These come in different formats, such as passports, birth certificates and drivers' licenses.

· **Proofs**: Showing that you hold the verifiable credential itself. This can be done by offering the verifiable credential such as a showing a driver's license. It can also be done by offering evidence that you have/hold a credential itself without showing the actual credential. This type of proof is referred to as "**zero knowledge proof**."

· **Verified Credentials:** A third party validates that according to their records, the claims are true.

· **Attester:** An issuer (which could be a third party such as a bank) issues a credential that says an individual has a bank account there. For instance, in the case

of a bank account, the Bank agrees and issues a credential that "attests" to the fact that the bank account is there. The Bank would be the Attester. Or, an individual can issue a credential that "self-attests" to the fact asked to be proven. The individual would then be the Attester.

C. Credential Issues with Centralized Identity Systems

Frequently in real life you routinely cannot provide just the relevant data needed to prove your identity when presenting a credential. For instance, presenting a Driver's License to gain access to a building provides more information to a security guard than simply you are who you say you are. By default, data is overshared and the building management's liability and risk increases as it has made itself a hacking target by holding this information.

D. Decentralized Identity is an Evolving Solution

In the near future, we can imagine a world where we have the technological, legal, and economic ability to reasonably share data for the services we want and recall further usage of it once the original shared purpose has been satisfied. In the above example, this would mean that only the data required to enter the building is shared, and that data is not allowed to be retained once you leave the building.

In all types of systems, we still have to accommodate the fact that traditional data on-boarding is necessary. Someone still has to collect and hold the data, offer it, and allow it to be used. But today's systems do not provide an automatic mechanism to protect shared data from further disclosure. Future decentralized systems can add that type of control which would be a vast improvement.

09

IF DATA SHARING CAN BE CHANGED TO FIT FOR ITS MOST NARROW PURPOSE, RESTORING DIGITAL TRUST AND REASONABLY ALLOCATING LIABILITY CAN OCCUR

It is exciting to see what is on the horizon. Approximately 86 major participants in the identity and technology space have joined together in a technologically focused consortium, the Decentralized Identity Foundation ("DIF"). Notably, FAANG and many smart device and financial service providers are not members. However, certain large technology and other enterprises such as Microsoft, IBM, Mastercard, Aetna, and Accenture are participating. DIF's mission is to develop the foundational elements necessary to establish an open ecosystem for decentralized identity and ensure interoperability. In short, decentralized identity technological solutions with concomitant standards are being built. To that end, the World Wide Web Consortium ("WC3") has a working group to address the standards for Decentralized Identifiers.

10

SELF-SOVEREIGN IDENTITY SYSTEMS MAY MINIMIZE DATA OVERSHARING

A. What is Self-Sovereign Identity?

In the self-sovereign identity vision, individuals and entities are enabled to create and manage their identifiers in a decentralized fashion, without relying on a third-party identity provider for validation. The system architecture is structurally set up to work from the perspective of the individual or the entity that is to be identified, and in the case of humans, is often anchored by unique biometric identifiers. It is unlike existing identity solutions that are structured from the perspective of the organization that provides an identifier and thus the law needs to be engineered to become more human-centered. Implicit in this vision is the idea that you show the minimum information needed to access products and services. This is closer to the way the offline world works.

Many of the proposed identity systems that are being developed incorporate blockchain technology. The protocols create frameworks for social trust. It is early days, but early days with promise. Last year, Microsoft launched its ION system for user controlled identities on the Bitcoin blockchain.

Late last year, Square released a Whitepaper describing a new decentralized protocol to enable trust using decentralized identity and verifiable credentials to "prove" the identity. It provided initial open-source code and will continue to release tools as the year progresses.

Practically speaking, these types of identity systems can work in the following way: your verifiable credentials are held by you on your phone or in your personal cloud. You, and not some third party, hold that data, and only you determine where it goes. You may offer up that data as proof to a third party to verify it, and you may put automated or manual rules in place that do not allow that third party to keep it.

11

GOVERNING PRINCIPALS OF IDENTITY

Some final words on Self-Sovereign Identity. Identity practitioners have suggested governing principals to reinforce that the individual is control of his identity. These include:

1. **Existence.** *Users must have an independent existence.*
2. **Control.** *Users must control their identities.*
3. **Access.** *Users must have access to their own data.*
4. **Transparency**. *Systems and algorithms must be transparent.* Note: To this end, the foundation of all technology solutions to enable SSI must be open source.
5. **Persistence.** *Identities must be long-lived.* Though note that newer proposals focus on single use or disposable identities. This principal is evolving.
6. **Portability.** *Information and services about identity must be transportable.*
7. **Interoperability.** *Identities should be as widely usable as possible.*
8. **Consent.** *Users must agree to the use of their identity.*
9. **Minimization.** *Data collection, use, and retention must be minimized.*
10. **Protection.** *The rights of users must be protected.*

12

SELF-SOVEREIGN IDENTITY HAS PLUSES AND MINUSES

Self-Sovereign Identity has both pluses and minuses for consumers and enterprise. Both legal and technological barriers exist today. The law would need to evolve in tandem with the technology and regulations would have to be enacted to empower this type of business process. With this type of identity system, control and responsibility are housed with the individual. Arguably, it places an extreme burden on the individual due to information, technological, and legal asymmetries.

Creating this new environment of digital trust is disruptive and could initially threaten current data-driven business models such as social media which rely on harvesting our data to create products and services. However, it can also help de-risk and provide ease of compliance in ensuring our data is not trafficked downstream. New offerings that are privacy preserving could be more profitable and are up for grabs. The real winners will be individuals and society overall.

13

CONCLUSION: PROTECT PRIVACY THROUGH LEGAL AND TECHNOLOGICAL MEANS

In our increasingly data-driven world, we must adopt strong protections that preserve our autonomy. Such protections are derived from both legal and technological frameworks. Legal protections can be created by establishing a comprehensive federal scheme that recognizes privacy as a fundamental right. A Digital Bill of Rights with strong enforcement provisions should be created. Technological solutions that are architecturally developed from the individual privacy point of view should mesh with new laws that support privacy as a fundamental right. These trust frameworks and types of decentralized/blockchain identity systems are evolving. Tensions between these new identity systems, *status quo* business models, and existing privacy and data protection laws will have to be resolved. However, these types of systems that support

privacy rights may encourage new and more profitable products and services while helping to restore a more equal balance of power between an individual and the service provider. Privacy is possible in the digital age. With legal and technological means working together, we can protect our right to be left alone.

CPI SUBSCRIPTIONS

CPI reaches more than **35,000 readers** in over **150 countries** every day. Our online library houses over **23,000 papers**, articles and interviews.

Visit **competitionpolicyinternational.com** today to see our available plans and join CPI's global community of antitrust experts.

CPI COMPETITION POLICY™ INTERNATIONAL