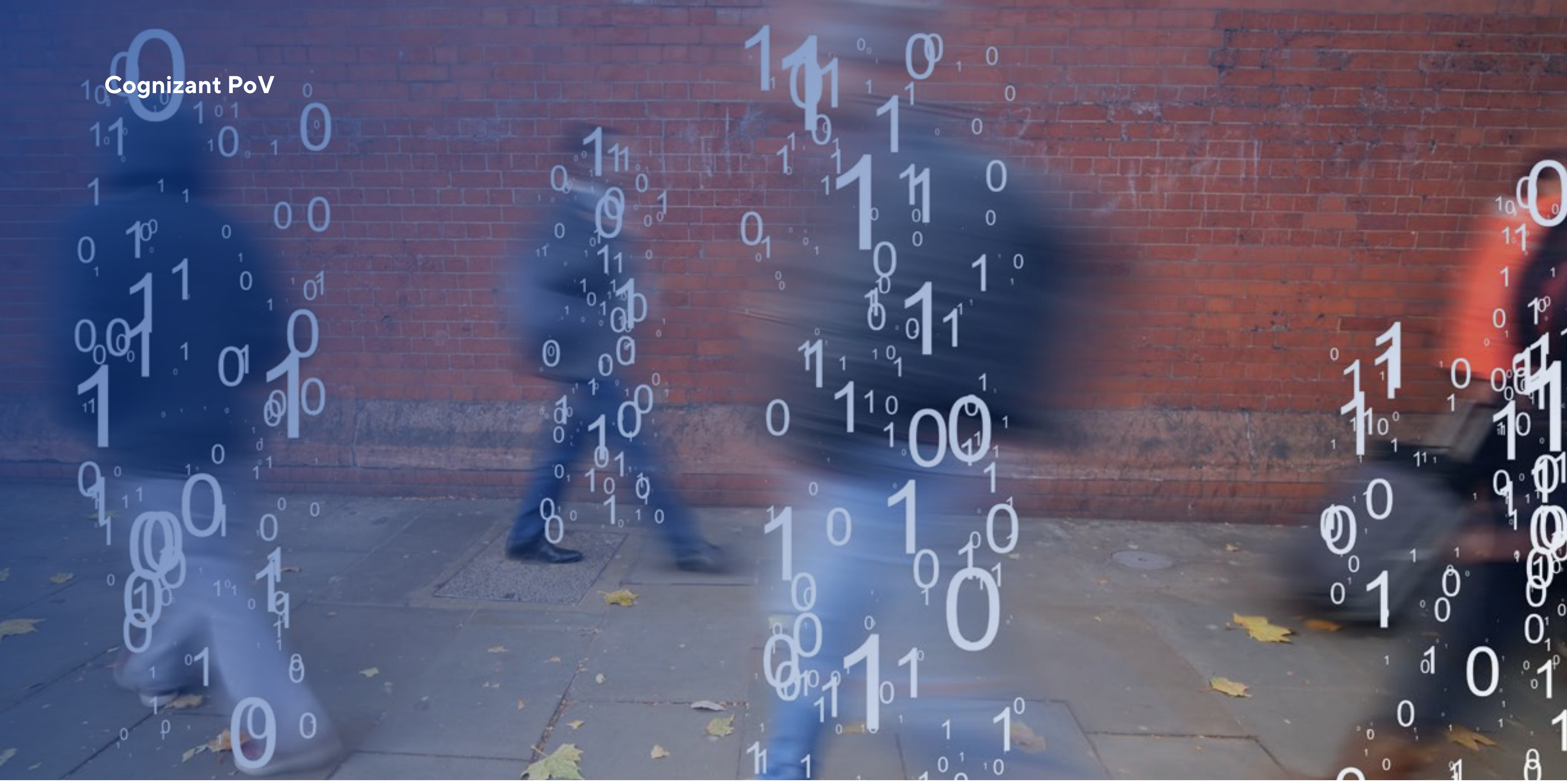


Digital Business

The Trust Paradox

As we face the end of old-world privacy, it’s time to take a hard look at what privacy and trust mean to us today.

By Paul Roehrig

Sorry to break it to you, but unless you’re reading this on parchment illuminated by a whale oil lantern, you’ve been hacked one way or another.

By “hacked,” we mean a cybersecurity breach or any other violation of personal data stewardship and governance that results in a breakdown of trust or privacy. These trust events are within the realm of cybersecurity but are also related to ethics, consumer attitudes, legislation, industry regulation and much more.

It’s no surprise that our new machines — Internet-enabled, AI-fueled — are at the center of redefining trust, transparency and privacy.

We now use the distant offspring of the original ARPANET to bank, manage our health, buy everything from real estate to charging cables, communicate socially and consume NAHRAH content (Netflix+Amazon+Hulu+Roku+Apple+HBO).

From these countless interactions, we create a “halo” of data that is every bit as real — and more monetizable, and steal-able — as our physical selves (which we discuss in our book *Code Halos*).[1] An unfortunate side effect is that now, if you have a password to *anything*, you are a user, a product *and* a target.

In spite of debates (and lawsuits, and arguments), however, we are making progress — recognizing our new issues, putting modern guiderails in place and debating what privacy and trust mean. But we have much left to do as we move into our new machine economy.

By 2021, the estimated impact of cybercrime alone, not including ruptured societies and nudged elections, will be around $6 trillion (more than the 2018 GDP of Japan).

The staggering reality of our online lives

There are literally dozens of mega-hacks, data breaches and — now — incidents of personal data misuse every year, and this is eroding our collective sense of privacy and trust in technology, the organizations with which we interact and even each other.

The numbers describing our machine-age lives are astronomic and math-phobia-inducing. Facebook has 1.28 billion active daily users.[2] Twitter hosts over 500 million tweets per day.[3] YouTube's popular T-Series channel, featuring Indian music, has more subscribers than the e*ntire population of Germany*.[4] All that money and information in transit makes attacking privacy and trust a profitable business.

According to Shape Security, in 2017 alone, 2,328,576,631 credentials — our username and password information — were "spilled."[5] (That's what the "boffins" call it.[6]) They also found that credential "stuffing" — using stolen data — accounts for 80% to 90% of retailer e-commerce logins.[7] By 2021, the estimated impact of cybercrime alone, not including ruptured societies and nudged elections, will be around $6 trillion (more than the 2018 GDP of Japan).[8] (And crime can pay. There's already an exchange-traded fund called HACK that outperforms the S&P 500 by focusing on cybersecurity companies.)

From crisis of trust to moment of reckoning

The daily barrage of news about intentional and unintentional use and misuse of our personal data has left many feeling vulnerable, used and even angry, and progress can seem maddeningly slow. The W3C's Tracking Protection Working Group simply shuttered in January 2019 after eight years of limited progress.[9] Then, just days ago, Apple removed the "Do Not Track" option from Safari to get a better view of our browsing habits.[10]

A boisterous — even rancorous — debate is gaining in volume and intensity in private companies, legislative halls, regulatory agencies, the media and around kitchen tables the world over, discussing the best way to manage trust and privacy in what the World Economic Forum calls the Fourth Industrial Revolution.[11]

We might think: If we're *all* hacked, there's no privacy anyway. *I'm* not rich or famous, and I'm a decent human, so what's the harm? We can't trust anything! What can I *do* about it anyway? I'm sure "they" will figure it out for us, right?

Well, no. The point is that if our personal information is used by a crook to buy jeans, that's bad, but it doesn't cause a seismic rift in our society. The *real* downstream impact of a lack of confidence in technology is that we're now facing a period of reckoning where we must wrestle with some fundamental questions that demand responses: What is true? Who can we trust? Who owns the digital me? Is privacy a right or a commodity?

What we say vs. what we do when it comes to trust and privacy

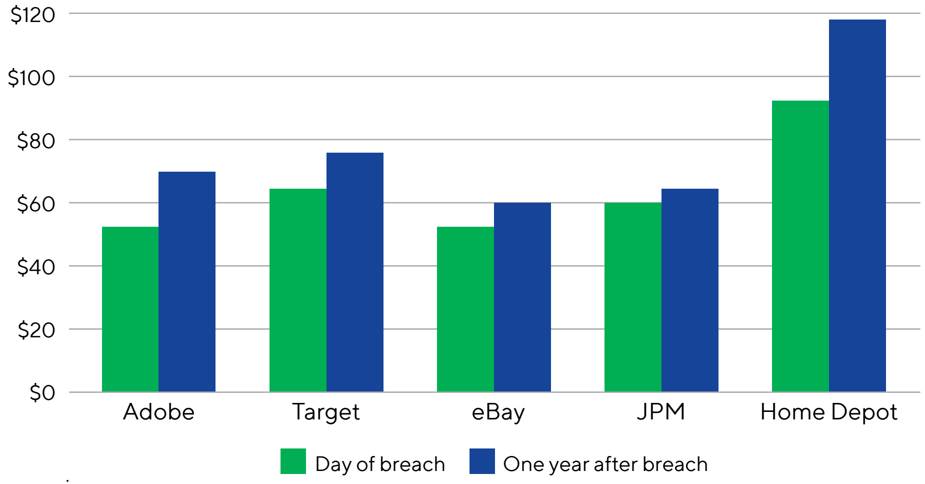
Even as consumers and politicians express outrage, our own behavior doesn't match our rhetoric. There's a real incongruity between what we say about security and trust and what we actually *do* about it.

Countless surveys have revealed essentially the same thing: When asked if trust matters, we all say yes! Our research found that 57% of Asia-Pac consumers would stop doing business with a company that has broken their trust.[12] We say we don't want to be tracked. In fact, only 17% of consumers in a recent study said personalized ads are even ethical.[13]

Even members of Gen Z — perceived to be completely *laissez-faire* with their information — are only slightly more liberal with their personal data, with 2019 Cognizant data showing that nearly 70% are "concerned that companies know too much about them."[14]

We consistently say we want privacy and that it matters whether we can trust a company or not, but when it comes to convenience and cost savings, we're actually pretty forgiving. Although we may rail at companies and bad actors, as well as regulators, our own social media behavior and Internet use hardly changes. In fact, although a mega-hack erodes trust, impacts stock valuation and — for a time — keeps people away, the reputational damage — and valuation impact — so far seems short-lived (see Figure 1).[15]

Per share price after data breaches



Source: *CSO* magazine
Figure 1

Even as consumers and politicians express outrage, our own behavior doesn't match our rhetoric. There's a real incongruity between what we say about security and trust and what we actually do about it.

What we know is this: In spite of trust and privacy concerns, humans simply are not coded to successfully avoid the rush we get from going online.

The truth about trust

Here's a hard truth: We are not going back. A handful of people may be able to unplug, but they are the outliers. You and I are not those people.

We haven't been willing to change behavior, even though there's a growing feeling (and science) that we're collectively moving in an unhealthy direction. This should be unsurprising. We eat sugar, smoke cigarettes, drink booze, burn hydrocarbons and eat mammals in spite of a mass of legitimate evidence confirming that none of these are "good for us."

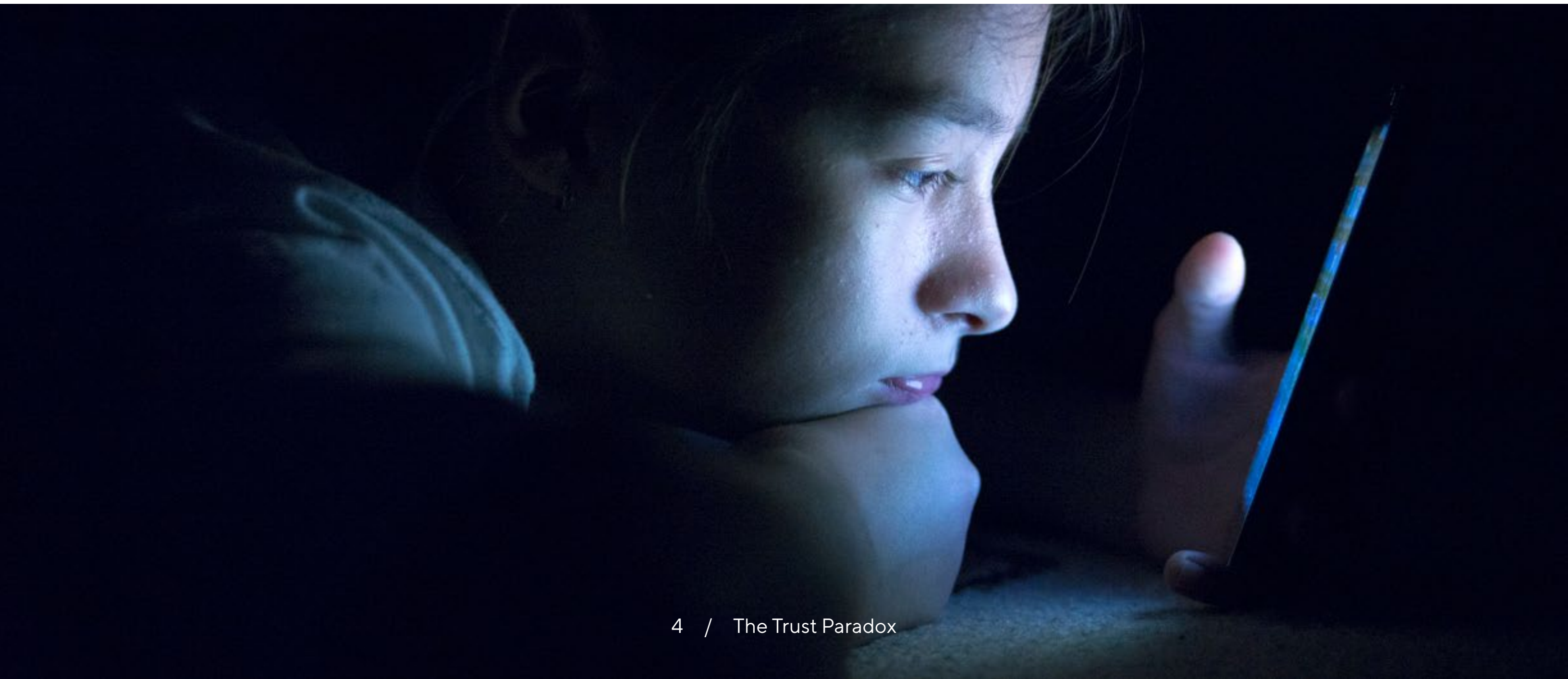
What we know is this: In spite of trust and privacy concerns, humans simply are not coded to successfully avoid the rush we get from going online. Our family, friends and associates, and the companies we deal with, are *not* going dark on the Internet either. Even for people who actually do try to quit a social media platform, a vast majority return.[16] (Not as high as the 90% relapse rate for smoking,[17] but it's a lot.)

We're rightfully concerned (or terrified) about trust, transparency and privacy, but we're not going to join a hunter-gatherer tribe that's sworn off *Fortnight*, Google and every IP-addressable thing.

Our new machine age is simply too enticing, profitable, interesting, addictive and fun.

For all of us, this means:

1. Technology is more central to *every* interaction.
2. Trust in *all* technology is eroding.
3. Because of this, trust seems to be draining from our social institutions and even personal relationships.
4. Our responses to this, so far, have been pretty anemic.



The future of trust and privacy

This puts us at a moment of reflection and inflection. What we decide about trust and privacy over the next couple of years will shape our economy and society for decades to come. We'll either find ourselves with a digital economy that is pure weaponized capitalism (where every click is monetizable unless you can afford to be "dark") or pure big brother authoritarianism (where content and clicks are tightly controlled) or (hopefully) something in the middle.

Oligarchs and autocrats may be fine with either of the endpoints on the spectrum. However, neither alternative will be attractive to most in a modern democratic society. As a result, we have a lot of work to do. The sea of unknowns and questions is vast:

- What is the future of trust? Of privacy?
- How should we govern and regulate data in an economy increasingly driven by new machines?
- How should companies be thinking about encoding greater protection into the technologies that the industry is developing and using?
- How can we foster trust in our institutions and even with each other?

> What we decide about trust and privacy over the next couple of years will shape our economy and society for decades to come.

The good news, and we should call it that, is we're now recognizing the problem. Clearly, that's the first step to making progress with a solution. Legislation such as GDPR in Europe is just the first necessary step needed as we renegotiate our terms of endearment with the new machines.[18] In fact, Facebook is now staring down the barrel of a multi-billion-dollar fine[19] by the U.S. related to potential privacy violations associated with Cambridge Analytica.[20]

Regardless of how this conundrum plays out, it's clear that modern democratic societies and forward-thinking companies are taking steps to apply new guardrails to data monetization, privacy and transparency to salvage trust in our increasingly digital interactions.

It's a lot to wrestle with, but there are a few certainties we can build on:

- **We must face the paradox.** Traditional ideas of trust, privacy and transparency simply don't hold up to the new machine promise. Hoping our conventional notions of privacy will suffice is naïve at best and, at worst, likely to be scarier and more dangerous for us all.
- **We need better rules** — via legislation, regulation and industry oversight — that encode the values — what we *really* want — of our civil societies. (What happens in the UK, China, South Africa, Russia, the U.S. and India will be, and should be, different.) Hiding from this, or trivializing how important it is, or letting individuals or even commercial organizations try to police this on their own is to abdicate our responsibilities and invite trouble into our homes and businesses.

- ***We* get to decide.** Things might feel a bit dire, but our current debates show democracy is working (slowly, where it's applied). We're fighting about trust and privacy and governance, which, in a healthy society, is what we're *supposed* to do. A little shouting is a positive sign. The end of old-school privacy is a hard thing to face, but *we* get to determine whether privacy is a right or a product that we have to pay for. *We* get to decide if a social credit score[21] is worth having. I think not, but you might; the point is, we get to work it out together.

We're in it together

It certainly won't be easy, but we needn't despair. We have remarkable new tools, huge oceans of data, capital, social constructs, intellectual property and structures of law. Most importantly, we have each other. Global-scale technology makes us more interdependent, so to manage trust and privacy we have to cooperate — even if we may not agree — or we all fail. This is a solid foundation for solving thorny problems.

In the end, the smart money is on humans making a mess of things at times but moving forward into a future that is *always* just a bit better.

Endnotes

[1] Malcolm Frank, Paul Roehrig and Ben Pring, *Code Halos: How the Digital Lives of People Things, and Organizations Are Changing the Rules of Business*, Wiley, 2014, www.cognizant.com/code-halos.

[2] "Facebook Statistics Directory," Social Bakers, www.socialbakers.com/statistics/facebook/.

[3] Twitter Usage Statistics, Internet Live Stats, www.internetlivestats.com/twitter-statistics/.

[4] Netflix's T-Series channel has 87 million subscribers, while Germany's population is less than 83 million.

[5] "2018 Credential Spill Report," Shape Security, http://info.shapesecurity.com/rs/935-ZAM-778/images/Shape_Credential_Spill_Report_2018.pdf.

[6] *Boffin* is a British slang term for a scientist, engineer, or other person engaged in technical or scientific research and development.

[7] Dennis Green and Mary Hanbury, "If You've Shopped at These 16 Stores in the Last Year, Your Data Might Have Been Stolen," Business Insider, Aug. 22, 2018, www.businessinsider.com/data-breaches-2018-4.

[8] Steve Morgan, "Cybercrime Damages $6 Trillion by 2021," Cybersecurity Ventures, Dec. 7, 2018, https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/.

[9] The W3C former Tracking Protection Working Group Charter website: www.w3.org/2016/11/tracking-protection-wg.html.

[10] Ahiza Garcia, "What Apple Killing Its Do Not Track Feature Means for Online Privacy," CNN Business, Feb. 13, 2019, www.cnn.com/2019/02/13/tech/apple-do-not-track-feature/index.html.

[11] "The Fourth Industrial Revolution," Klaus Schwab, World Economic Forum, www.weforum.org/about/the-fourth-industrial-revolution-by-klaus-schwab.

[12] "The Business Value of Trust," Cognizant, May 2016, www.cognizant.com/whitepapers/the-business-value-of-trust-codex1951.pdf.

[13] John Koetsier, "Only 17% of Consumers Believe Personalized Ads Are Ethical, Survey Says," *Forbes*, Feb. 9, 2019, www.forbes.com/sites/johnkoetsier/2019/02/09/83-of-consumers-believe-personalized-ads-are-morally-wrong-survey-says/amp/.

[14] "Gen Z: The World by the Thumbs," Cognizant and The Center for Generational Kinetics, March 2019.

[15] Doug Drinkwater, "Does a Data Breach Really Affect Your Firm's Reputation?" *CSO*, Jan. 7, 2016, www.csoonline.com/article/3019283/does-a-data-breach-really-affect-your-firm-s-reputation.html.

[16] Araceli Cruz, "Farewell Facebook, and Good Riddance," ABC News, March 7, 2013, https://abcnews.go.com/ABC_Univision/quitting-facebook/story?id=18668978.

[17] Matt Sailor, "How Often Do Smokers Relapse When They Quit?" How Stuff Works, https://health.howstuffworks.com/wellness/smoking-cessation/how-often-do-smokers-relapse.htm.

[18] "Every Move You Make: Privacy In the Age of the Algorithm," Cognizant, May 2018, www.cognizant.com/whitepapers/every-move-you-make-privacy-in-the-age-of-the-algorithm-codex3684.pdf.

[19] Tony Romm, "The U.S. Government and Facebook Are Negotiating a Record, Multibillion-dollar Fine for the Company's Privacy Lapses," *The Washington Post*, Feb. 14, 2019, www.washingtonpost.com/technology/2019/02/14/us-government-facebook-are-negotiating-record-multi-billion-dollar-fine-companys-privacy-lapses/?noredirect=on&utm_term=.b0542e27cef3.

[20] Alix Langone, "Facebook's Cambridge Analytica Controversy Could Be Big Trouble for the Social Network," *Time*, April 4, 2018, http://time.com/5205314/facebook-cambridge-analytica-breach/.

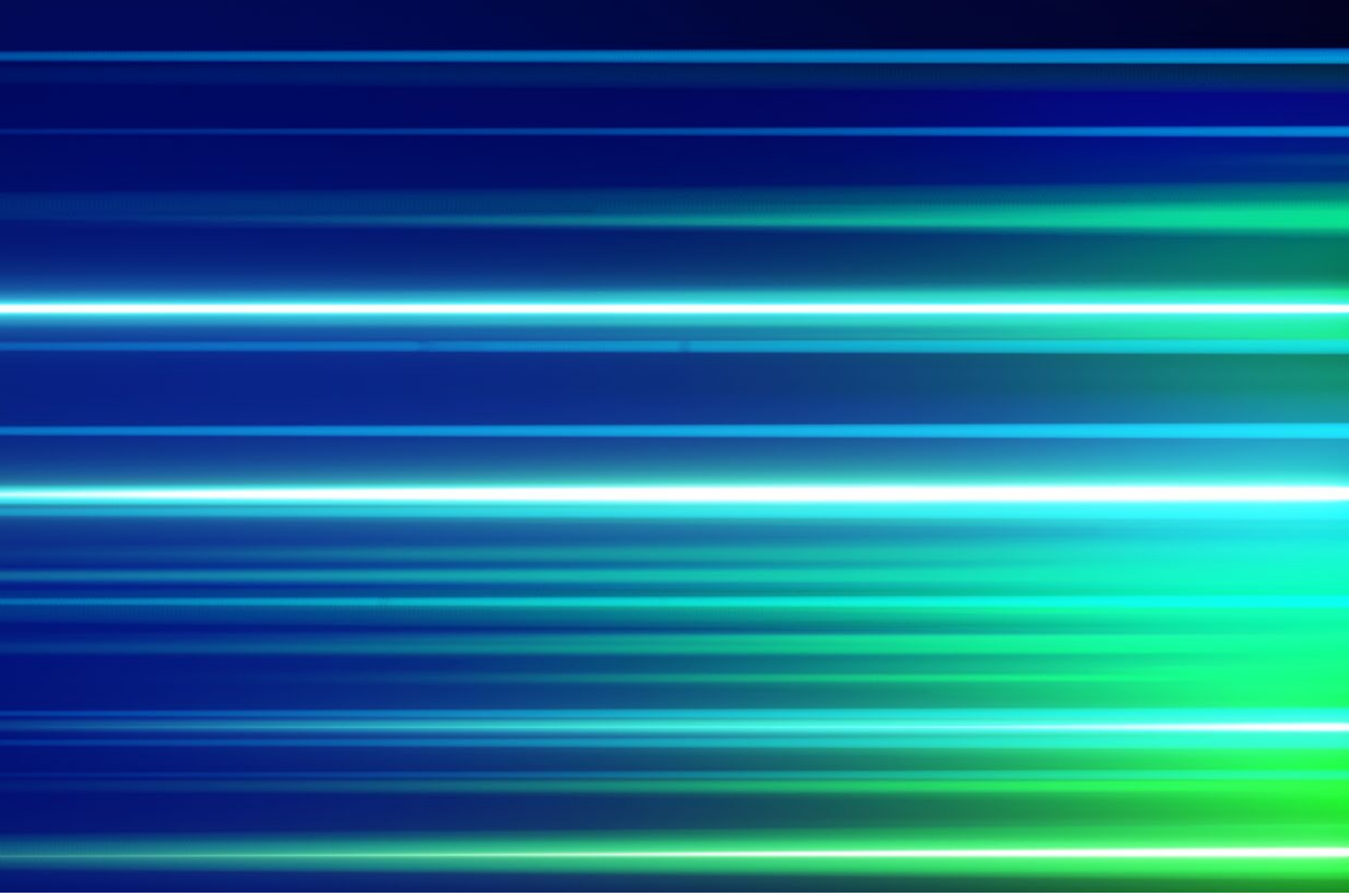
[21] "China Assigns Every Citizen a 'Social Credit Score' to Identify Who Is and Isn't Trustworthy," CBS New York, April 24, 2018, https://newyork.cbslocal.com/2018/04/24/china-assigns-every-citizen-a-social-credit-score-to-identify-who-is-and-isnt-trustworthy/.

About the author

Paul Roehrig

Head of Strategy, Cognizant Digital Business

Paul Roehrig is Head of Strategy for Cognizant Digital Business. He is the founder and former Global Managing Director of Cognizant's Center for The Future of Work. Along with Malcolm Frank and Ben Pring, he is a co-author of *What To Do When Machines Do Everything: How to Get Ahead in a World of AI, Algorithms, Bots, and Big Data* and *Code Halos: How the Digital Lives of People, Things, and Organizations are Changing the Rules of Business*. He can be reached at Paul.Roehrig@cognizant.com | www.linkedin.com/in/paul-roehrig-020785/.



About Cognizant Digital Business

Cognizant Digital Business helps our clients imagine and build the Digital Economy. We do this by bringing together human insight, digital strategy, industry knowledge, design, and new technologies to create new experiences and launch new business models. For more information, please visit www.cognizant.com/digital or join the conversation on LinkedIn.

About Cognizant

Cognizant (Nasdaq-100: CTSH) is one of the world's leading professional services companies, transforming clients' business, operating and technology models for the digital era. Our unique industry-based, consultative approach helps clients envision, build and run more innovative and efficient businesses. Headquartered in the U.S., Cognizant is ranked 195 on the Fortune 500 and is consistently listed among the most admired companies in the world. Learn how Cognizant helps clients lead with digital at www.cognizant.com or follow us @Cognizant.

World Headquarters

500 Frank W. Burr Blvd.
Teaneck, NJ 07666 USA
Phone: +1 201 801 0233
Fax: +1 201 801 0243
Toll Free: +1 888 937 3277

European Headquarters

1 Kingdom Street
Paddington Central
London W2 6BD England
Phone: +44 (0) 20 7297 7600
Fax: +44 (0) 20 7121 0102

India Operations Headquarters

#5/535 Old Mahabalipuram Road
Okkiyam Pettai, Thoraipakkam
Chennai, 600 096 India
Phone: +91 (0) 44 4209 6000
Fax: +91 (0) 44 4209 6060

Codex 4455