Do Online Access Imperatives Violate Duty of Care?

Stephen Cobb

This article presents four assertions: (1) going online exposes us to a lot of crime, (2) high crime environments are unhealthy, (3) governments and companies that make us go online may be breaching their duty of care, (4) there is an urgent need to reduce cybercrime and support cybercrime victims.

An illustration of the way in which going online exposes us to crime

"Just go online" is a three-word phrase we hear a lot these days. We hear it from government agencies, utilities, healthcare providers, educational institutions, and just about every commercial entity with whom we do business. Just go online to get information, support, customer service. Just go online to pay bills, complete forms, answer questions. Just go online to apply for benefits, subsidies, assistance, etc.

Sadly, there's nothing "just" about just going online these days. I firmly believe that to go online in 2023 is to expose oneself to a wide range of criminal activity, from a diverse array of frauds and scams to identity theft and financial loss, not to mention stalking, profiling, and harassment.

I say this as someone who has a master's degree from a well-regarded school of criminology, someone who has worked in cybersecurity for more than 30 years. Computer-enabled crime is as old as computers, but it has been growing rapidly over the last 20 years. The reality today is that you become a target for criminals as soon as you get a smartphone or tablet or laptop computer.

Indeed, some of those devices come with malicious code pre-installed. All of them come with an email address or phone number that criminals can probe for weaknesses, be they digital or psychological.

How bad has digitally enabled crime become? In the UK, the National Crime Agency says, "Fraud remains the most common crime type experienced by victims in England and Wales," noting that "Data breaches continue to be a key enabler of fraud." The British House of Lords has said that "an adult aged 16 or over in England and Wales is more likely to become a victim of fraud than any other individual crime type."

In America, after surveying US adults earlier this year, the AARP found that: "Scams—and seemingly constant scam attempts by phone, email and text—have grown so pervasive, two-thirds of Americans say they're at a crisis level."

One leading indicator of online fraud activity is phishing attacks, defined by the Anti-Phishing Working Group (APWG) as "a crime employing both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials." APWG has been around for 20 years. In the first quarter of 2023, APWG observed 1,624,144 phishing attacks, noting: "This is a record high—the worst quarter for phishing that APWG has ever observed."

The graph below charts the accelerating year-on-year increase in the amount of money people have lost to Internet crime this century, as reported to the FBI's Internet Crime and Complaint Center. (I am aware of, and had written extensively on, the problems inherent in measuring cybercrime, but I'm satisfied that this curve reflects the trend in online criminal activity.)

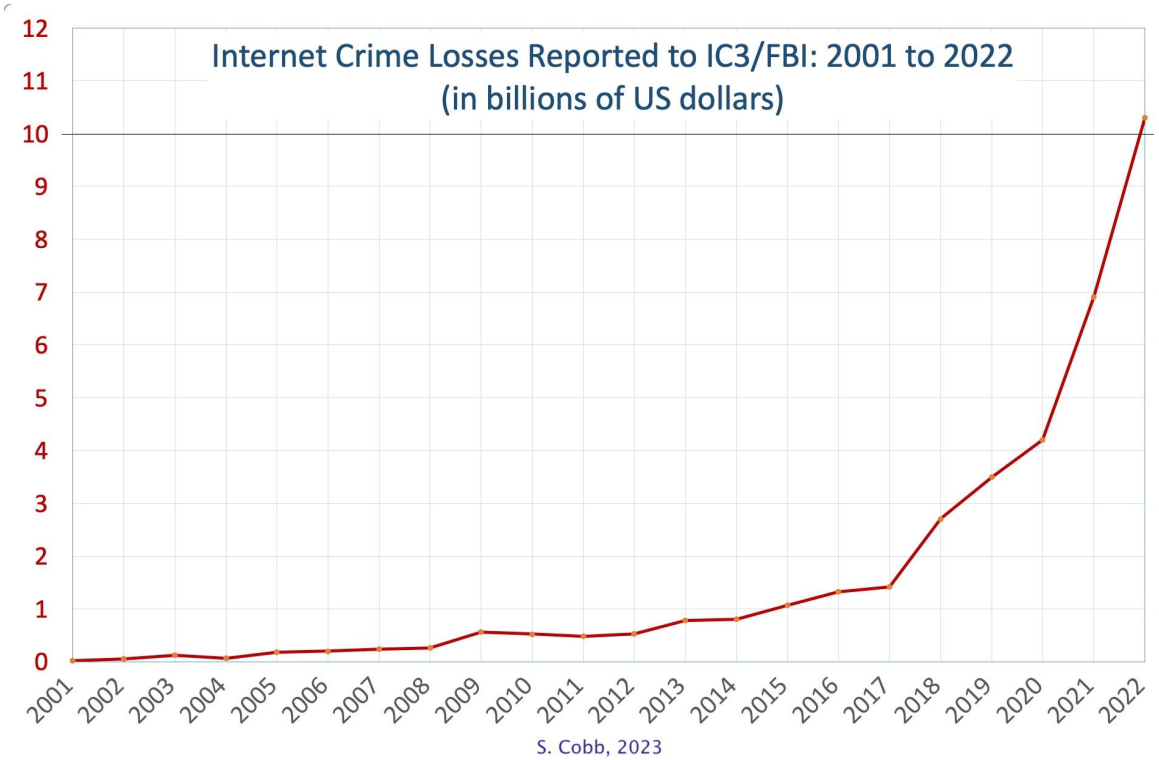


Chart showing the growth of cybercrime as reflected in Internet crime losses, 2001 to 2022

Subjective well-being, life satisfaction, and social value

As you can see, in just seven years Internet crime losses rose 10X, from $1 billion on 2015 to over $10 billion in 2022. However, bad as those numbers are, they only capture one part of the impact of online crime: financial loss from victimization.

In fact, Internet fraud has a more costly impact than just financial loss. This was firmly established by Modal and Anderson in their 2015 article: *It's All Over but the Crying: The Emotional and Financial Impact of Internet Fraud*. As they put it: "Internet fraud's emotional impact is a major component of victimization and felt as strongly as the financial impacts."

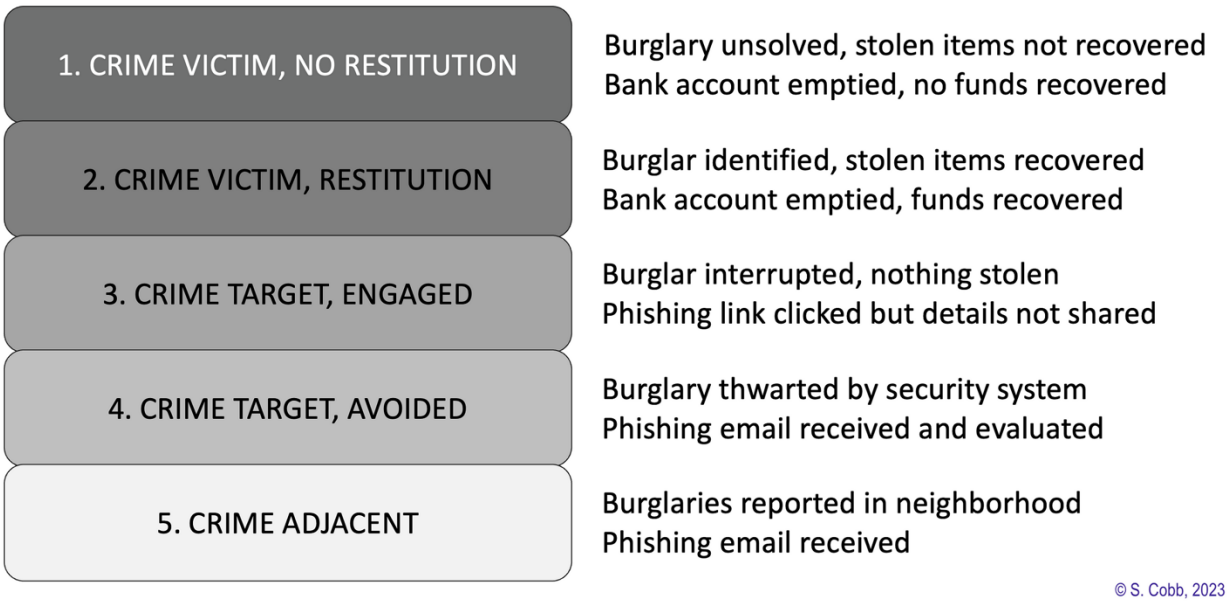
I saw proof of that assertion about seven years ago when a colleague in America was hit by tax refund fraud, a digitally-enabled crime that I detailed in this article in 2016. What is revealing about this crime is that victims don't lose money, technically speaking they "just" experience a delay in receiving money, namely, their expected income tax refund.

For many US households this refund is thousands of dollars and normally received soon after filing your annual income tax returns. Families figure this predictable financial event into their annual budgeting, but if digital scammers file a fake return in your name, the money can be delayed by six months or more (in 2016 the average delay was 278 days).

The effect of this crime on my colleague was, in his words, deeply unsettling. Even though he had not lost any money, he seriously questioned his faith in people, government, and other institutions (his family's private information had been exposed in a major data breach at a large health insurance company). Back then I was not familiar with the concepts of *subjective well-being*, *life satisfaction,* and *social value*. But in hindsight I can see that, as a victim of digitally-enabled fraud, my colleague took a big hit to all three.

Social value, subjective well-being, and life satisfaction are part of a system of metrics that can be used to calculate the impact of online fraud on victims. Through social value studies we are learning that the harm to fraud victims is often greater than their financial loss, as much as 4X in one major study (see my talk on this in June, 2023). Furthermore, such studies can put a value on the hit we take from crimes even when we don't lose any money.

We need more research on social value right across what I see as the five levels of impact from predatory crimes. To be clear, these are the levels of harm as I see them, others may see more or less. These levels exist for both traditional (meatspace) crimes and digitally-enabled (cyberspace) crimes. Here's a rough diagram of how I see the five levels, with level one being the worst, and level five being the least worst, although not without harm:



I will explain how even level five—being adjacent to crime—can cause harm, after looking at how we can attach a value to level one, where the fraud victim loses money and doesn't get it back. Recently, a company that specializes in social value studies, Simetrica-Jacobs, worked with the UK consumer watchdog Which? to monetize the change in life satisfaction associated with being scammed. They found that "fraud victims would require £2,509 ($3,150) of extra income, on average, to have a level of life satisfaction equivalent to what would be expected had the person not been scammed." This study was conducted, "Following best-practice guidance from HM Treasury … and using an unbiased estimate of the impact of income on one's life satisfaction (Fujiwara & Dass, 2021)."

The Simetrica-Jacobs-Which research strongly indicates that "the average fraud victim would require £2,509 to compensate them for the loss in wellbeing that's associated with being scammed." The study found that this was true of both offline and online fraud, with some indications that the latter may cause even more harm, "broadly in line with the impact of being threatened" (see Scams and Subjective Wellbeing, 2021).

Harm caused by exposure to crime

But wait, there's more. As many readers may know—from direct experience or that of friends and family—we don't have to lose money to a criminal to suffer harm. Being targeted by criminals can also take a toll on both our mental and physical health. The same is true of having to spend time adjacent to crime (level one). Simply being exposed to crime has negative health effects.

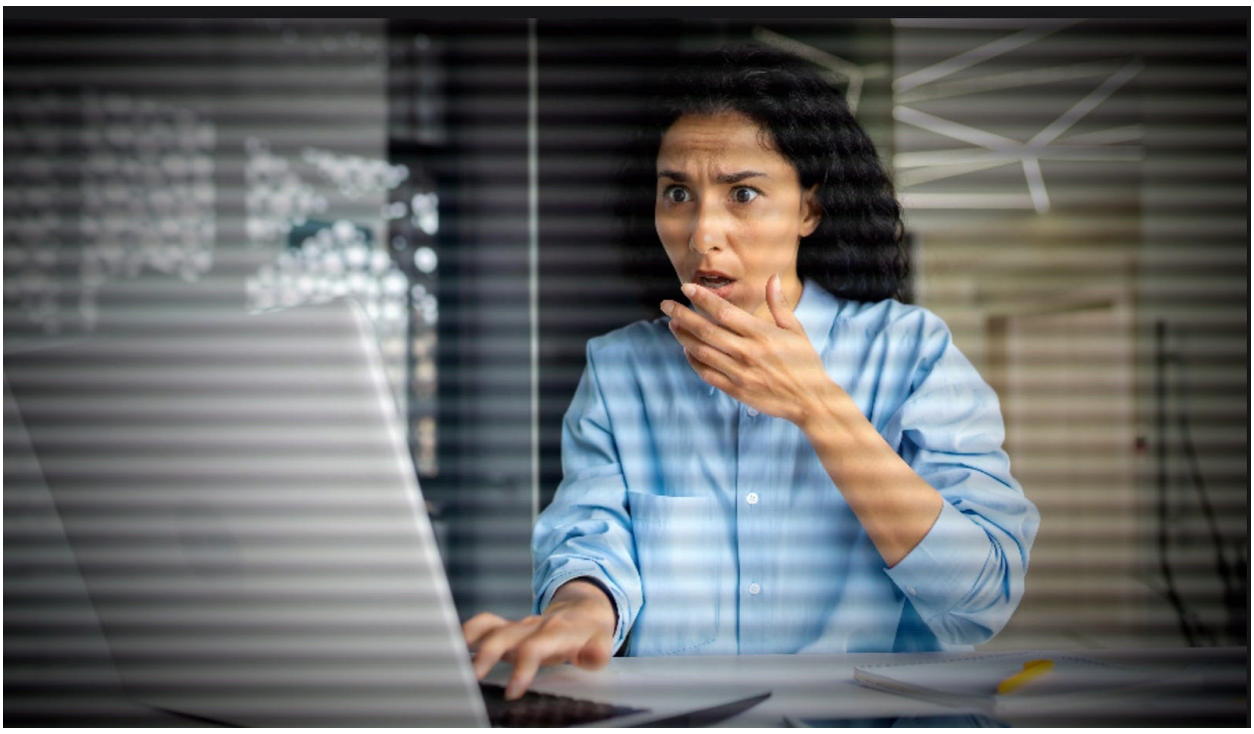
We know this because exposure to traditional crime has been widely studied by criminologists and other social scientists, as well as epidemiologists and population health experts. This is evident when you google the words 'health in high crime neighborhoods.' Last time I did that, the first search result was this: "Studies have indicated neighborhood crime can harm health even

among people not directly impacted by the violence. Potential long-lasting effects include increases in blood pressure and obesity, both risk factors for cardiovascular disease."

That's a quote from: "*The Ripple Effect of Neighborhood Crime: When Crime Decreases, So Do Cardiovascular and Coronary Artery Disease Mortality Rates."* The article was written by Lauren Eberly, MD, MPH, and Sameed Khatana, MD, MPH, of the University of Pennsylvania. The same authors, plus seven more, wrote "*Association Between Community Level Violent Crime and Cardiovascular Mortality in Chicago: A Longitudinal Analysis*," published in the *Journal of the American Heart Association* in July of 2022.

When it comes to mental health, here's a snippet from "*The impact of neighbourhood crime on mental health: A systematic review and meta-analysis*," by Gergő Baranyi et al.: "living in a high crime area exposes residents to increased social stress linked to mental health through biological mechanisms by disrupting the hypothalamic- pituitary-adrenal axis regulating the stress response (Do et al., 2011), or by causing systematic inflammation in the body (Nazmi et al., 2010)."

In my opinion, spending time in a high crime environment is demonstrably bad for both our mental and physical health; and there's a chunk of solid, peer-reviewed science to back that up. You can find it by using Google Scholar to look up health in high crime neighborhoods. Also, at the end of this article I have listed dozens of academic papers on this topic.



Stock photo from Pond5, illustrating distress when going online

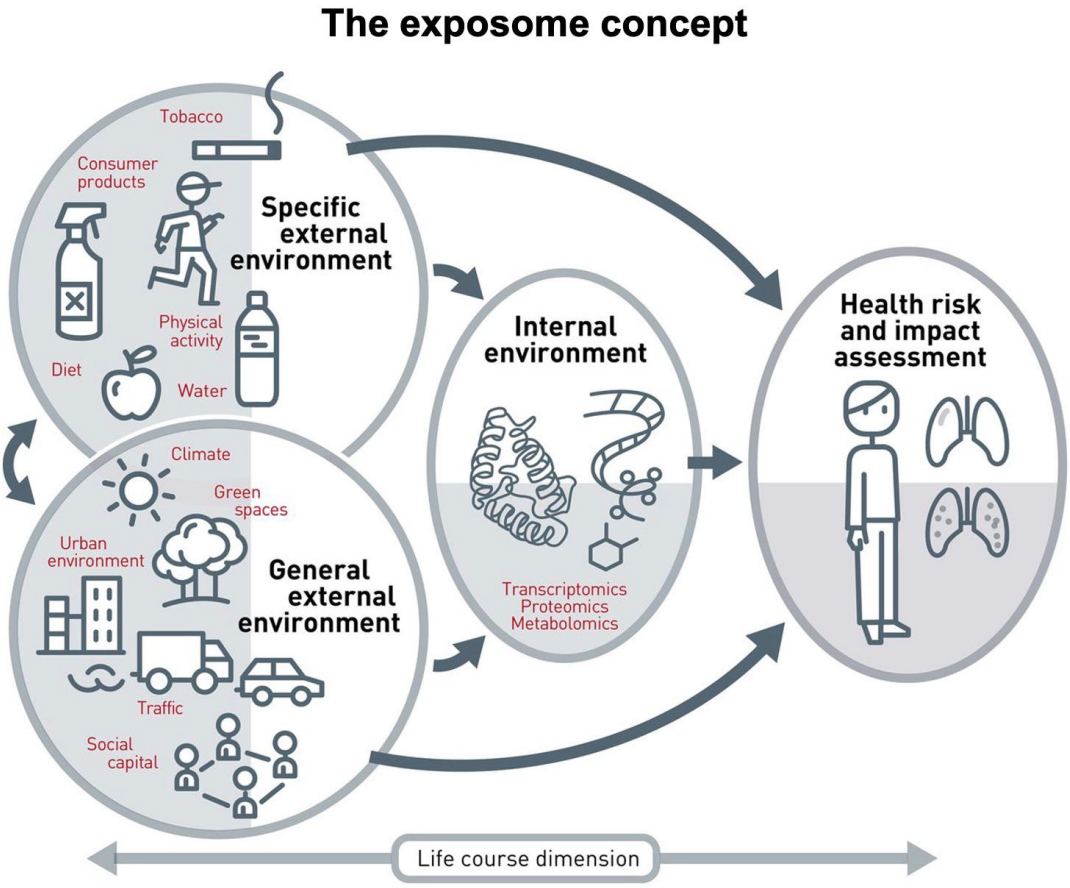
Enter the exposome

In light of the above, and the research that I have done around the epidemiological concept of the *exposome*, I believe that "just going online" is bad for human health.

Exposome is a term used "to describe environmental exposures that an individual encounters throughout life, and how these exposures impact biology and health." (Wikipedia). The following is a useful introduction to the exposome from a 2017 journal article, *The exposome and the future of epidemiology: a vision and prospect*:

"It is widely accepted that a relatively small proportion of chronic disease can be explained by genetic factors alone. Although information about environmental exposure is important to comprehensively evaluate chronic diseases, this information is not sufficiently or accurately assessed by comparison with genomic factors. To emphasize the importance of more complete evaluation of environmental exposure, the concept of the exposome, which indicates the entirety of environmental exposure from conception onwards, was introduced in 2005." (Environmental Analysis, Health and Toxicology, Kyoung-Nam Kim and Yun-Chul Hong, 2017.)

The diagram below, by Martine Vrijheid, Research Professor and Head of the Environment and Health over the Lifecourse Programme at the Barcelona Institute for Global Health, may help you visualize the exposome. You can see that it encompasses exposures in both our internal and external environment, with the latter consisting of general and specific environments (see *The exposome: a new paradigm to study the impact of environment on health*, 2014.)



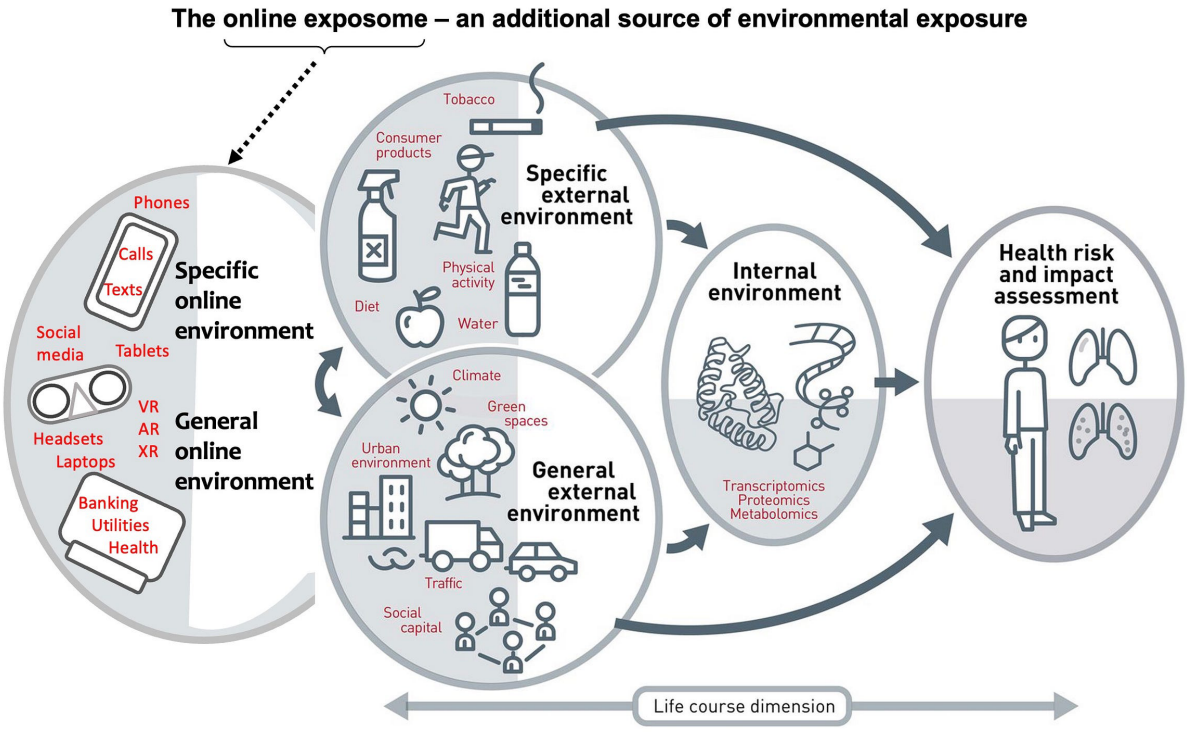
Martine Vrijheid, *Thorax* 2014;69:876-878

The concept of the exposome illustrated by Martine Vrijheid in Thorax journal, 2014;69:876–878, Copyright © BMJ Publishing Group Ltd & British Thoracic Society. All rights reserved.

The online exposome

A key role of the exposome is to help us acknowledge and account for everything to which we are exposed in our daily lives that may affect our health. The article quoted earlier by Kim and Hong puts it like this: "The exposome encompasses not only environmental chemicals and pollutants but also lifestyle, socioeconomic status, social capital and the social environment, and even biological responses."

For me, it's clear that everything to which we are exposed by "being online" is part of the exposome. I've taken the liberty of expanding Prof. Vrijheid's illustration to help visualize this. My crudely drawn icons on the left represent smartphones, tablets, VR headsets, laptops and desktop computers, devices on which many people spend many hours every day in a range of activities that expose them to crime.



The online exposome, added to an illustration of the exposome by Martine Vrijheid

When I first read about the exposome, I thought the term "digital exposome" would be a good way to refer to the digital environment we inhabit when we "go online." Not surprisingly, I was not the first person to think of this term. For example, it appears in a 2017 article from *Studies in Health Technology and Informatics*: "In an increasingly digitised world more attention should be paid to the digital component of the exposome derived from the interactions of individuals with the digital world. We define this "Digital Exposome" as the whole set of tools and platforms that an individual uses and the activities and processes that an individual engages with as part of his/her digital life." (G. Lopez-Campos et al., 2017)

While I strongly agree with the gist of that article, I have also found *digital exposome* used in other ways, for example, to describe the use of digital tools to record pollution exposure in the general and specific external environment (think personal air quality monitoring devices and so on).

I propose *online exposome* as a more appropriate term for "the set of tools and platforms that an individual uses and the activities and processes that an individual engages with as part of his/her digital life." The online exposome would thus include using a smartphone or other Internet-connected device, having an email address and one or more online accounts, and engaging digitally with individuals or organizations.

The online exposome as high crime neighbourhood

I am confident in asserting that the online expose is, in some significant ways, similar to a high crime environment. However, there are some serious differences between living in a high crime neighbourhood in meatspace and going online.

For a start, it can be harder—in some ways—to get out of being online than it is to move out of a high crime neighbourhood (and I say this fully mindful of how socio-economic factors can trap people in disadvantaged locations). Consider what it takes to get to a point where online crime is no longer a concern.

People use terms like "going offline" or "disconnecting" when they forsake their screens for the weekend, or leave phones and computers at home when they go on vacation. But our online presence persists even when we're not logged on, and unless we are good at compartmentalizing, so does the stress of knowing that our digital identity can be stolen and abused while we're offline (it can even be hacked and hijacked after we're dead). To truly go offline means closing accounts, erasing profiles, deleting cloud storage and all the data entities have stored about you as a result of your online interactions.

To be clear, I'm not advocating that we should all go offline. There are many genuine benefits to being online. But I would argue that it's getting increasingly difficulty to enjoy those benefits without being exposed to the harmful effects of criminal activity. At the same time, many of the entities that benefit from us going online are failing to do all they can to make it a safe and healthy place to be.

It should also be noted that some "benefits" of going online feel so good they are addicting, further complicating efforts to manage exposure to the online exposome. Intentional fostering of online addiction for profit is now at the center of some big lawsuits and I am hopeful these cases will lead to positive changes. However, I also think regulation of online technologies is needed at the national and international level. Absent such interventions, the future deployment of increasingly immersive technologies will make going online even more addictive, a prospect my good friend Winn Schwartau explores in his forthcoming book: The Art and Science of Metawar: How to Survive AI-Driven Reality Distortion, Disinformation, Manipulation, & Addiction in the Metaverse.

Duty of care when saying "go online"

Both professionally and personally, I see the online exposome as highly criminogenic, that is: "causing or likely to cause criminal behaviour." Indeed, many countries devote an entire month each year to raise everyone's awareness of all the things one needs to do, or not do, in order to avoid becoming a victim of online crime (I mean Cybersecurity Awareness Month). And every day of the year we are warned and reminded, both online and off, that cyber-criminals are out to get us, to take our money and data, to access our accounts and devices.

For me, all of the above raises the following question: If an entity requires a person to go online, do they have a duty of care to that person when they do go online? I think the answer is yes. Entities that require a person to go online have a responsibility, a duty of care, to protect that person from the harms they may suffer from being online. I also think that the current high levels of digitally-enabled crime mean that many institutions are in breach of this duty of care.

In my opinion, there is an urgent need for all countries to address the detrimental effects of their citizens going online. Globally, the number of hours per day that working age Internet users spend online is currently somewhere between six and seven hours (DataReportal). By going online we add another dimension to our total environmental exposure, one that contains considerable potential for harmful effects on our health.

Think about being on a crowded underground train, a part of your general external exposome. You are exposed to bacteria, viral diseases, and air pollution. You are also exposed to pickpockets and stalkers. It's not exactly a healthy environment. Now you take out your smartphone and go online. Sadly, you are now exposed to criminal activity on top of all the other potentially harmful exposures (as I attempted to illustrate at the top of this article).

Clearly, there are many reasons why governments need to do more to reduce cybercrime; but, as far as I can tell, protecting the health of the country's population has not yet been accepted as one of those reasons. That needs to change, starting now. The benefits of online technology are being undermined by the harmful effects of going online. Furthermore, absent serious intervention, going online is likely to become an even more immersive experience, expanding the amount of time we spend online and—without serious online crime reduction—the range of crimes to which we will be exposed.

Summary

Hopefully, some legal experts out there will read this article and be inspired to pursue litigation based on the information that I have laid out. For example, they could develop cases that confirm a duty of care arising from online imperatives, achieving settlements that push governments and companies to either drop "go online" requirements or do more to make going online less harmful. At the same time, legislation is needed to acknowledge the full range of harms suffered by victims of cybercrime, along with adequate funding of victim support to minimize the short- and long-term impact of those harms on individuals, families, and society at large.

In closing, if you think this article makes a good case for one or more of my four assertions, please share it with others:

1. *Going online exposes us to a lot of crime*. We see criminal activity all around us, coming at us through emails, texts, social media posts, malicious advertising, poisoned search results, and so on. Phishing attacks and losses to Internet crime are at record levels.
2. *High crime environments are unhealthy.* We see multiple studies showing that exposure to crime, online as well as offline, has harmful impacts on mental and physical health, individually and across society.
3. *Governments and companies that make us go online may be breaching their duty of care*. We see people going online because some entities force them to do so, even though those entities know that going online exposes people to harms and victimization against which there is currently inadequate protection.
4. *More must be done to reduce cybercrime and support cybercrime victims*: We see the current situation causing multiple preventable harms and seriously undermining the benefits of current and future technologies.

Notes:

A. This article is based on a talk I was going to give at a conference in Barcelona in November, 2023. Unfortunately, my partner's health made attending that event impractical. Hopefully, I will have an opportunity to present the talk somewhere, at some point. By then I will have added another section addressing the inequity factor at the nexus of online access imperatives and cybercrime harms. (There are multiple socio-economic barriers to "just going online," often summed up as the digital divide. This exists in every country; for example, 20% of UK adults lack basic digital skills, a situation vigorously addressed by this UK charity.)

B. I am grateful to Foy Shriver and Peter Cassidy of APWG for encouraging my research. I love the title that Peter proposed for my talk: *Are Online Access Imperatives Going to Make Us Sick*? I particularly liked, and have adopted, the excellent phrase: "Online Access Imperatives."

C. I apologize for mixing UK and US English in the text, but if you hear me deliver this content as a talk, you will hear an unintentional blend of UK and US accents, with Americans telling me I sound British and Brits telling me I sound American. (If I record a reading of this article, I will post a link here and you can hear for yourself.)

D. Lawyers in America should explore and/or sponsor the research I have referenced on the non-financial harms caused by online crime; then they should mount fresh attacks on the inhuman and illogical US court rulings that insist—in the face of common sense and lived experience—that having one's data privacy breached by criminals causes no serious harms aside from material losses for which victims have receipts.

E. Here's a link to Google Search results around the health effects of exposure to crime.

F. Below is a list of article titles from my somewhat informal review of the literature, with apologies for lack of links, authors, publications, etc. I just don't have the time right now to make this a more formal References list. That said, even a quick scan of these titles gives you an idea of how much work has been done on the effects of exposure to crime.

1. Neighborhood violent crime and perceived stress in pregnancy
2. Crime, neighborhood deprivation, and asthma: a GIS approach to define and assess neighborhoods
3. Residence in high-crime neighborhoods moderates the association between interleukin 6 and social and nonsocial reward brain responses
4. High Crime Neighborhoods as a Driver for Toxic Stress Leading to Asthma
5. Neighborhood crime and depressive symptoms among African American women: Genetic moderation and epigenetic mediation of effects
6. Pathways to depression: The impact of neighborhood violent crime on inner-city residents in Baltimore, Maryland, USA
7. Neighborhood crime-related safety and its relation to children's physical activity
8. Social connection to neighbors, multiple victimization, and current health among women residing in high crime neighborhoods
9. Neighborhood stressors and cardiovascular health: Crime and C-reactive protein in Dallas, USA
10. Differences by race in the associations between neighborhood crime and violence and glycemic control among adults with type 2 diabetes
11. High-crime neighborhoods as a war zone: comparing trauma as a result of war and neighborhood violence
12. The association between experiences of being defrauded and depressive symptoms of middle-aged and elderly people: a cross-sectional study in China
13. Impact of self-reported bank fraud on self-rated health, comorbidity and pain
14. Not a victimless crime: The impact of fraud on individual victims and their families
15. Increasing cybercrime since the pandemic: Concerns for psychiatry
16. Corruption, fraud and cybercrime as dehumanizing phenomena
17. E-fraud: Exploring its prevalence and victim impact
18. Exploring how, why and in what contexts older adults are at risk of financial cybercrime victimisation: A realist review
19. Smartphone addiction and cybercrime victimization in the context of lifestyles routine activities and self-control theories: The user's dual vulnerability model of cybercrime victimization
20. The" Right to Control" Theory of Fraud: When Deception without Harm Becomes a Crime
21. Denying victim status to online fraud victims: the challenges of being a 'non-ideal victim'
22. The reporting experiences and support needs of victims of online fraud
23. Cybercrime: A new and growing problem for older adults
24. Criminals work from home during pandemics too: A public health approach to respond to fraud and crimes against those 50 and above
25. The role of health concerns in phishing susceptibility: Survey design study
26. Globalization and cybercrimes: A review of forms and effects of cybercrime in Nigeria
27. COVID-19 and cyber fraud: Emerging threats during the pandemic
28. Cyberchondria, Coronavirus, and Cybercrime: A Perfect Storm
29. Social networks as predictors of the harm suffered by victims of a large-scale Ponzi scheme
30. Challenges of responding to online fraud victimisation in Australia
31. Improving the police response to online fraud
32. Exploring fear of crime for those targeted by romance fraud
33. Responding to individual fraud: Perspectives of the fraud justice network
34. Identity theft and fraud victimization: What we know about identity theft and fraud victims from research-and practice-based evidence

35. Fraud and its relationship to pandemics and economic crises: From Spanish flu to COVID-19
36. Medicare beneficiaries' exposure to fraud and abuse perpetrators
37. Impact of applying fraud detection and prevention instruments in reducing occupational fraud: case study: Ministry of Health (MOH) in Gaza strip
38. COVID-19 and organized crime: strategies employed by criminal groups to increase their profits and power in the first months of the pandemic
39. Violent crime and outdoor physical activity among inner-city youth
40. The psychological and financial impact of cybercrime victimization: A novel application of the shattered assumptions theory