REMOTE WORKERS, EVER-PRESENT RISK: EMPLOYER LIABILITY FOR DATA BREACHES IN THE ERA OF HYBRID WORKPLACES

David Garrison Golubock[*]

ABSTRACT

The years since the onset of the COVID-19 pandemic have seen explosive growth in the number of remote workers, and companies have struggled to cope with a perceived loss of productivity and establish reliable methods of remote access to cope with this influx. At the same time, the last few years have seen a continued rise in the threat of data breaches, as sophisticated groups of malicious actors have targeted businesses and governments, locking systems with ransomware and exposing sensitive company data and employees' personal information. This article aims to examine the intersection between these two trends, examining how an employer's policies for enabling remote work and monitoring remote employees can significantly impact the employer's potential liability in the event of a data breach. After surveying the current state of remote work and data breach law, this article examines the potential interplay between remote work and a data breach in a private company through a series of linked hypotheticals, closing with proposals for legislative reform to ensure greater data security and practical recommendations for employers seeking to mitigate the risks created by a remote workforce.

[*] David Garrison Golubock is an Assistant Attorney General in the Environmental & Public Protection Division of the Vermont Attorney General's Office. This article represents his own views, not those of the Vermont Attorney General's Office. The author thanks Daniel Hemel, Neil Cohen, Justin Kolber, Marsha Garrison, and Chief Judge Nancy J. Rosenstengel for their insightful comments on early drafts of this article.

REMOTE WORKERS, EVER-PRESENT RISK: EMPLOYER LIABILITY FOR DATA BREACHES IN THE ERA OF HYBRID WORKPLACES

TABLE OF CONTENTS

INTRODUCTION

A classic case found in many law school torts textbooks, *The T.J. Hooper* tells the tale of an entire industry bluntly told by the judicial system that its manner of operating is antiquated and that it must pay damages for failing to adopt a revolutionary new technology with sufficient alacrity.[1] In his decision issued in 1932, Judge Learned Hand held tugboat owners to account for failing to equip their vessels with radios, a new technology that had only recently become available to regular businesses and consumers.[2] "[I]n most cases reasonable prudence is in fact common prudence" Judge Hand wrote, yet in many cases, "a whole calling may have unduly lagged in the adoption of new and available devices . . . Courts must in the end say what is required; there are precautions so imperative that even their universal disregard will not excuse their omission."[3]

Over the last decade, not merely a single industry but the entire economy has realized that it has lagged in adopting adequate cybersecurity in the face of the growing threat of data breaches. Recent years have seen increasingly sophisticated malicious actors use clever social engineering to circumvent the most sophisticated security systems, causing billions of dollars in damage.[4] Legislators, enforcers, and courts have all scrambled to create a new body of law that can assess what measures are adequate in a rapidly evolving cybersecurity landscape.

At the same time, the last few years have seen an explosion of remote work. While the technology that supports remote work may have existed for a decade or more, until the onset of the COVID-19 pandemic, these technologies were seen as tools to increase efficiency, allowing employees to expand work hours to home time and permitting more accessible work while traveling.[5] Only a privileged few employees could obtain long-term, fully or predominantly remote positions, and these often came with trade-offs, putting

[1] 60 F.2d 737 (2d Cir. 1932).

[2] *Id.* at 739–40.

[3] *Id.* at 740.

[4] Tim Maurer & Arthur Nelson, *The Global Cyber Threat*, IMF (Spring 2021), https://www.imf.org/external/pubs/ft/fandd/2021/03/global-cyber-threat-to-financial-systems-maurer.htm [https://perma.cc/JUB4-B667].

[5] Morris Davis & Andra Ghent, *Work From Home: How COVID-19 Sped up the Inevitable*, WORLD ECON. F. (Apr. 22, 2021), https://www.weforum.org/agenda/2021/04/technology-wfh-work-home-covid19/ [https://perma.cc/3KRY-MNEN].

employees on some kind of 'flex track' that might provide lower compensation or fewer opportunities for advancement.[6]

Since the onset of the COVID-19 pandemic in 2020, everything has rapidly and dramatically changed.[7] As employees spend more time on company systems at home, professional and personal boundaries have inevitably blurred, and high percentages of employees have reported using company devices for personal purposes.[8]

Employers have been somewhat unwilling participants in this shift towards remote work —while some have simply tried to convince or coerce employees to return to the office, others have accommodated remote work while trying to find ways to ensure that remote workers remained productive. Some employers have turned to measures described as "employer surveillance," which may include active monitoring of employee screens and keystrokes, giving employers powerful abilities to observe employee activities and catch "inefficient" employees while vastly diminishing employee privacy and sending a message that the employer is literally always looking over one's shoulder.[9]

Much has already been written about the implications of employer surveillance in the era of remote work, and many commentators have already decried employer efforts to monitor remote workers as a significant invasion of employee privacy.[10] This paper does not intend

---

[6] NICHOLAS BLOOM, HOW WORKING FROM HOME WORKS OUT, STAN. INST. ECON. POL'Y RSCH. (June 2020); Sabrina Wulff Pabilonia & Victoria Vernon, *Telework, Wages, and Time Use in the United States*, GLOB. LAB. ORG. DISCUSSION PAPER, NO. 970 (July 27, 2021); Brett Christie, *Stunted Growth: Remote Work's Effect on Career Development*, WORLDATWORK: WORKSPAN DAILY (Mar. 25, 2022), https://worldatwork.org/resources/publications/workspan-daily/stunted-growth-remote-work-s-effect-on-career-development [https://perma.cc/5XLK-QA8D].

[7] Davis & Ghent, *supra* note 5.

[8] Shweta Sharma, *Your Employees are Using Sensitive Corporate Devices for Personal Browsing*, CSO ONLINE (Mar. 28, 2024), https://www.csoonline.com/ [https://perma.cc/DP9J-LDYM].

[9] Stephen J. Malone et al., *Monitoring Remote Employees*, REUTERS: PRACTICAL LAW THE JOURNAL (Oct. 2023), https://www.reuters.com/practical-law-the-journal/transactional/monitoring-remote-employees-2023-10-02/ [https://perma.cc/YR6U-F2T7]; Thorin Klosowski, *How your Boss Can Use your Remote-Work Tools to Spy on you*, N. Y. TIMES: WIRECUTTER (Feb. 10, 2021), https://www.nytimes.com/wirecutter/blog/how-your-boss-can-spy-on-you/ [https://perma.cc/67F5-W6JB].

[10] *See, e.g.*, Tammy Katsabian, *The Telework Virus: How COVID-19 has Affected Telework and Exposed its Implications to Privacy*, 44 BERKELEY J. EMP. & LAB. L. 141 (2023); *see also* Richard A. Bales & Tammy Katsabian, *The Invisible Web at Work: Artificial Intelligence and Electronic Surveillance in the Workplace*, 41 BERKELEY J. EMP. & LAB. L. 1 (2020).

to rehash discussions of the ethics and privacy implications of employer surveillance. Rather, it proposes that the limited focus on willful surveillance by employers overlooks the much broader risks associated with the greater access to employee data that most employers assume, whether intentionally or not, simply by enabling remote access to employer systems from devices that are increasingly used for personal purposes as well as business. Remote access becomes a virtual umbilical cord that connects employers to their employees, enabling the modern reality of remote work but creating new risks in the event of a significant data breach.

This article will examine the interplay between modern remote work and data breaches, outlining how an employer's choices in creating remote access can significantly impact potential liability in the event of a data breach. This article will assess the current landscape of remote work, using contemporary statistics to discuss the prevalence of remote work, the types of devices used for remote work, and the instrumentalities employers use to permit remote access. The article will then describe the realities of modern data breaches and outline the law governing liability for data breaches. The article will then use a series of linked hypotheticals to illustrate how different choices made by a company in creating remote access for employees can result in dramatically different outcomes in the event of a data breach, potentially exacerbating the employer's liability. The article will conclude with practical recommendations for how companies can seek to mitigate the risks associated with data breaches in the context of remote work, as well as outline legislative steps that lawmakers should take to incentivize businesses to make responsible choices.

I. REMOTE WORK

A. The Current Landscape of Remote Work

While its precise origin is hard to pinpoint, remote work is a very recent phenomenon as it exists in the marketplace today.[11] Employers indeed have, to some extent, permitted employees to complete certain tasks at home since at least the beginning of the Industrial Revolution, when entrepreneurs using the "putting out" system permitted individuals to produce goods such as textiles and leather goods at home rather than traveling to a

[11] *A Brief History of the Workhome*, WORKHOME, http://www.theworkhome.com/history-workhome/ [https://perma.cc/K25A-WGPX] (last visited on Apr. 1, 2024); *see also* Pabilonia & Vernon, *supra* note 6.

central factory.[12] But this phenomenon utilized individuals more as contractors, who independently engaged in tasks with little communication between themselves or the main employer, rather than in today's closely connected remote workplace.[13]

The modern foundation of remote work came with the advent of technologies such as the fax machine and modern pre-digital telephonics, which enabled features such as voicemail and the conference call by the 1970s.[14] The combined power of these technologies allowed some white-collar employees to at least contemplate the possibility of working remotely while staying connected to coworkers in the office, exchanging written documents, and participating in meetings. The possibility of remote work came to appear as particularly desirable in the wake of the 1973 OPEC oil embargo, when rapidly increasing gas prices made commuting costly and led to national initiatives to reduce automobile use.[15] Further impetus in favor of remote work came through the Americans with Disabilities Act in 1990 and additional regulations from the EEOC, as remote work offered a way to accommodate certain classes of employees without expensive changes to the structure of a business's physical office space.[16] In 1996, even the federal government began pushing for greater remote work, using new technologies such as the internet and email to create the

[12] Maxine Berg, *Factories, Workshops and Industrial Organisation*, *in* AN ECONOMIC HISTORY OF BRITAIN SINCE 1700, VOL. 1 1700-1860 127–28 (R.C. Cloud & D.N. McCloskey ed., 1994); Alice Littlefield & Larry T. Reynolds, *The Putting-Out System: Transitional Form or Recurrent Feature of Capitalist Production?*, 27 SOC. SCI. J. 359–72 (1990).

[13] Littlefield & Reynolds *supra* note 12.

[14] The fax machine was invented in 1964 and became common office equipment by the late 1970s, while teleconferencing first appeared in 1956 and voicemail appeared in the late 1970s. *See, e.g.*, Linsey Knerl, *When Was the Fax Machine Invented?*, HP (Dec. 7, 2019), https://www.hp.com/us-en/shop/tech-takes/when-was-fax-invented [https://perma.cc/7E3V-8BR2]; *The History of Voicemail*, VOX SCIENCES, https://www.voxsci.com/cms/showPage?PAGE=voicemailHistory.tml [https://perma.cc/6HTS-8KWS] (last visited Oct. 7, 2023); *Evolution of the Conference Call*, RINGCENTRAL, https://www.ringcentral.com/gb/en/blog/the-evolution-of-the-conference-call/ [https://perma.cc/GA4Z-LF3R] (last visited Oct. 7, 2023).

[15] *See, e.g.*, Vicky Gan, *What Telecommuting Looked Like in 1973*, BLOOMBERG (Dec. 1, 2015), https://www.bloomberg.com/news/articles/2015-12-01/what-telecommuting-looked-like-in-1973; [https://perma.cc/8MMU-9ZMN]; Prithwiraj Choudhury, *Our Work-from-Anywhere Future*, HARV. BUS. REV. (Nov. – Dec. 2020), https://hbr.org/2020/11/our-work-from-anywhere-future [https://perma.cc/J9U6-ED7U].

[16] Choudhury, *supra* note 15; Ravi S. Gajendran & David A. Harrison, *The Good, the Bad, and the Unknown About Telecommuting: Meta-Analysis of Psychological Mediators and Individual Consequences*, 92 J. APPLIED PSYCH. 1524, 1524 (2007).

National Telecommuting Initiative, which aimed to have as many as 160,000 federal employees working remotely at least some of the time by 2002.[17]

Indeed, the Internet and the advent of reasonably priced personal computers and laptops truly advanced the possibilities of remote work, allowing for vastly easier document sharing and communication. These capabilities were further enhanced by rapidly increasing internet speeds – global average internet speed leaped from only 127 kbps in 2000 to as much as 4.4 Mbps in 2010, a roughly 34-fold increase that enabled easy video conferencing and permitted reliable access to cloud-based files and applications.[18] Global average internet speed had grown to as much as 52.9 by 2019 on the eve of the Covid-19 pandemic.[19]

By the late 2010s, all the pieces were in place to enable white-collar professionals to work remotely with ease and seamlessly communicate with coworkers: cloud-based document management systems, applications, remote desktops, easy video conferencing, and plentiful cheap laptops, monitors, and webcams. The spread of remote work was slow, but even prior to the pandemic, employees had begun pushing for greater remote work options, mostly not seeking to work remotely full-time but embracing remote work as a way to gain greater flexibility rather than having a mandatory physical presence in an office for 40 hours a week.[20] Employers permitted remote working arrangements as a means of improving employee productivity and retention.[21] But the spread of remote work pre-pandemic was nonetheless slowed by employers who resisted the expansion of remote

[17] Tom Shoop, *That Time Even Minimum Telework Was Viewed with Wonder and Fear*, GOVERNMENT EXECUTIVE (May 12, 2023), https://www.govexec.com/management/2023/05/time-even-minimum-telework-was-viewed-wonder-and-fear/386267/ [https://perma.cc/3DAT-GGJ8].

[18] CISCO, *Annual Cisco Visual Networking Index Forecast Projects Global IP Traffic to Increase More Than Fourfold by 2014* (June 2, 2010), https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2010/m06/annual-cisco-visual-networking-index-forecast-projects-global-ip-traffic-to-increase-more-than-fourfold-by-2014.html [https://perma.cc/5VLZ-HHSM].

[19] CISCO, CISCO ANNUAL INTERNET REPORT 2018–2023, 15 (Mar. 9, 2020).

[20] *See, e.g.*, Niraj Chokshi, *Out of the Office: More People Are Working Remotely, Survey Finds*, N.Y. TIMES (Feb. 15, 2017), https://www.nytimes.com/2017/02/15/us/remote-workers-work-from-home.html [https://perma.cc/U6UN-FQLS].

[21] Brit Morse, *Study: Remote Workers Are Happier, Stay in Their Jobs Longer, and Work More Hours Than Onsite Employees*, INC. (Sept. 18, 2019), https://www.inc.com/brit-morse/remote-work-survey-owl-labs.html [https://perma.cc/3Q7N-VX7A].

work, insisting that in-person work resulted in greater creativity and collaboration.[22] In part, this opposition was simply cultural – older baby boomers were highly resistant to remote work, and the prevalence of baby boomers in management roles likely contributed to (and continues to contribute to) efforts to limit remote work opportunities.[23] Despite this opposition, remote work gradually became more common in the decade before the pandemic, with as many as 43 percent of Americans spending some time working remotely in 2017[24] and roughly half of US companies permitting employees to work remotely in 2018.[25]

This opposition rapidly disappeared when confronted with the reality of the COVID-19 pandemic in 2020 – as US states shut down in a wave in March 2020, tens of millions of workers found themselves working remotely by default full-time, and employers across the country were forced to cope.[26] Tools such as Zoom became household names overnight, while employers who lacked systems for remote access by employees scrambled to put them in place quickly.[27] Far from creating chaos, workers across the globe found that with fast internet and modern tools, they could work productively from home.[28]

---

[22] Mike Elgan, *Why Total Bans on Remote Work Don't Remotely Work*, COMPUTERWORLD (June 24, 2017), https://www.computerworld.com/article/3203249/why-total-bans-on-remote-work-dont-remotely-work.html [https://perma.cc/Y4M6-KJCH]; Yuki Noguchi, *Some Employers Are Rethinking Telework, Citing a Need for Better Collaboration*, NPR (Jul. 11, 2017), https://www.npr.org/sections/alltechconsidered/2017/07/11/535398716/some-employers-are-rethinking-telework-citing-a-need-for-better-collaboration [https://perma.cc/U2ZA-Q43X].

[23] *See, e.g.*, Quentin Fottrell, *Why Baby Boomers don't Like to Work from Home*, MARKETWATCH (Feb. 3, 2015), https://www.marketwatch.com/story/why-baby-boomers-dont-like-to-work-at-home-2015-02-03 [https://perma.cc/6L9P-WF7J].

[24] Chokshi, *supra* note 20.

[25] Rebecca Corliss, *More Than Half of Companies Surveyed Allow Remote Work, but Fast-Paced Industries Lag Behind*, ENTREPRENEUR (Oct. 29, 2018), https://www.entrepreneur.com/growing-a-business/more-than-half-of-companies-surveyed-allow-remote-work-but/322418 [https://perma.cc/2F8D-W4JU].

[26] Ben Casselman et al., *Who Still Works from Home?*, N.Y. TIMES (Mar. 8, 2024) https://www.nytimes.com/interactive/2024/03/08/business/economy/remote-work-home.html [https://perma.cc/G4A6-MKAY].

[27] *See, e.g.*, Alex Webb, *We Really Weren't Ready to Work from Home*, BLOOMBERG (Apr. 27, 2020), https://www.bloomberg.com/view/articles/2020-04-27/coronavirus-employers-scramble-to-get-to-grips-with-zoom-slack?ref=riskmarketnews.com [https://perma.cc/QFE5-7U8C].

[28] Jose Maria Barrero et al., *The Evolution of Work from Home*, 37 J. ECON. PERSPECTIVES 23, 25 (Fall 2023).

Post-COVID, the prevalence of remote work has regressed somewhat from its peak in the pandemic, but it remains widespread. A Pew Research Center study published in March 2023 found that roughly 35% of workers with jobs that can be done remotely (41% of total jobs) are working from home full-time.[29] The same survey found that 41% of those with jobs that can be done remotely are working a hybrid schedule.[30] And employees seemed enthusiastic about the prospect of increased remote work—the Pew study found that over 80% of hybrid employees would prefer to do even more of their work remotely.[31]

These findings are consistent with other surveys—a monthly survey run by researchers from the University of Chicago, ITAM, MIT, and Stanford found that at the end of 2023, around 29% of total paid full days across US households in the survey's target population were working from home, an increase of more than 300% since pre-Covid.[32] The survey found that employees hoped to work remotely close to three days per week on average, while surveyed employees indicated that on average their employers planned to permit only two days of remote work per week.[33] Of all the full-time employees surveyed, 12.4% were fully remote, 58.1% were entirely in-person, and 29.5% were in a hybrid arrangement.[34] Of those able to work remotely, 46.8% were in a hybrid arrangement, while 19.6% were fully remote.[35] Gallup's yearly "State of the Global Workplace" for 2023 found even higher rates of remote work, with 30% of the survey population exclusively remote and 24% in a hybrid arrangement.[36]

It is difficult to accurately survey employees across the entire economy, and the rapidly evolving landscape of remote work means that any survey results should be viewed with some skepticism. However, all signs indicate that there has indeed been a substantive shift towards much greater rates of remote work even after the lockdowns of the COVID-19 pandemic have receded. To assess the impact of this increase in remote work on employer

[29] Kim Parker, *About a Third of U.S. Workers Who Can Work from Home Now Do So All the Time*, PEW RSCH. CTR. (Mar. 30, 2023), https://www.pewresearch.org/short-reads/2023/03/30/about-a-third-of-us-workers-who-can-work-from-home-do-so-all-the-time/ [https://perma.cc/V99R-5Y2R].

[30] *Id.*

[31] *Id.*

[32] *See* JOSE M. BARRERO, NICHOLAS BLOOM & STEVEN J. DAVIS, WHY WORKING FROM HOME WILL STICK, NAT'L BUREAU OF ECON. RSCH. WORKING PAPER 28731 (Jan. 18, 2024), for the relevant SWAA January 2024 Updates (as cited in Barrero, *supra* note 28 at 25).

[33] *Id.* at 8.

[34] *Id.* at 12.

[35] *Id.* at 13.

[36] GALLUP, STATE OF THE GLOBAL WORKPLACE: 2023 REPORT 14 (2023).

vulnerabilities and data breaches, the key question to ask is how employees work remotely. This question is best resolved in two parts: what devices are employees using to work remotely, who do those devices belong to, and how are those devices being used, and what systems are employers using to enable remote access to employer data? These questions will both be examined in turn.

B. Devices Used for Remote Work

By far, the most prevalent device used for remote work is the computer. Of workers who relied on a technical device of some kind for their work, 96.7% reported using a desktop computer or laptop, according to a survey of 1,013 individuals by software developer Beyond Identity.[37] After laptop computers, mobile phones take a close second as the next most utilized device, with 66% of individuals reporting smartphone use for work according to Beyond Identity, or more than 80% in a different survey conducted by Zipdo.[38]

In the early days of the digital workplace, an employee was most commonly expected to use an employer-provided desktop computer in the employer's office.[39] When cheap laptops led many employers to issue laptops instead of desktop computers, these devices were still primarily intended to be used in the physical office, placed in a company-provided laptop dock—though the size of the laptop did allow for theoretical flexibility and the possibility of occasional work while traveling.[40] Similarly, as smartphones quickly revolutionized mobile phones in the 2000s, some employers initially focused on company-issued phones, gravitating towards devices such as the now-antiquated Blackberry that were seen as productivity-focused and more secure.[41]

---

[37] *BYOD: Exploring the Evolution of Work Device Practices in a New Remote-Forward Era*, BEYOND IDENTITY (May 28, 2021), https://www.beyondidentity.com/blog/byod-exploring-evolution-work-device-practices-survey [https://perma.cc/A8NK-TGCD].

[38] *Id.*; *see also Essential Smartphone in the Workplace Statistics in 2023*, ZIPDO, https://zipdo.co/statistics/smartphone-in-the-workplace/ [https://perma.cc/6AK9-X27M] (June 22, 2023).

[39] Owen Williams, *Thinner and Lighter Laptops Have Screwed Us All*, VICE (Jul. 24, 2018, 8:00 AM), https://www.vice.com/en/article/9kmkve/thinner-and-lighter-laptops-have-screwed-us-all [https://perma.cc/9TFG-AS28].

[40] *See generally Id.*; Sean Gallagher, *The Old Way of Handing out Corporate Hardware Doesn't Work Anymore*, ARS TECHNICA (Nov. 16, 2020), https://arstechnica.com/information-technology/2020/11/future-of-collaboration-04/ [https://perma.cc/Z4CZ-SM64].

[41] *See, e.g.*, Andres Martinez, *Once Upon a Time, We All Wanted A Blackberry. Remember?*, TIME (Oct. 1, 2013), https://ideas.time.com/2013/10/01/once-upon-a-time-we-all-wanted-a-blackberry-remember/;

Eventually, as laptops became a commonplace household item for most professionals, some companies instituted "bring-your-own device" policies for cost savings, requiring employees to use their own personal laptops for work rather than issuing company computers.[42] With the increase in remote and hybrid work arrangements following the pandemic, laptops have become the norm across businesses, and BYOD systems have become increasingly common for both laptops and smartphones.[43] Exactly how common is unclear, though the limited selection of data available on the subject indicates that around half of employers use personal computers for work – Beyond Identity's 2021 survey on BYOD practices found that 50.5% of employees at least sometimes use personal devices for work, with 14.4% only using personal devices.[44] Similarly, another 2021 survey conducted by cybersecurity provider Morphisec that specifically focused on remote workers found that 49% of those surveyed used personal laptops or computers, a figure that was down from 57% at the beginning of 2020.[45] This figure seems potentially much higher for smartphones – only a small number of employers ever used employer-issued phones, and the use of personal phones for work had become the norm even by 2016, when a study conducted by Tenable found that 72% of employers permitted or required some use of personal mobile devices for work.[46] A 2018 study by Samsung found that only 17% of companies provided employees with a work-issued smartphone, with 83% of employers permitting or requiring some use of personal mobile devices.[47] Statistics measuring the progression of this trend after the COVID-19 pandemic appear to be scarce and unreliable. Still, the general trend toward an increase in BYOD practices suggests that the number of individuals using personal phones for work continues to rise.

[https://perma.cc/T3V9-SER7]; N.Y. Times Editors, *Your Boss and Your BlackBerry*, N.Y. TIMES (Dec. 21, 2009), https://archive.nytimes.com/roomfordebate.blogs.nytimes.com/2009/12/21/your-boss-and-your-blackberry/ [https://perma.cc/7E9P-23C7].

[42] *See, e.g.*, Jeff Jones, *Beginner's Guide to BYOD (Bring Your Own Device)*, MICROSOFT (Jul. 17, 2012), https://www.microsoft.com/en-us/security/blog/2012/07/17/beginners-guide-to-byod-bring-your-own-device/ [https://perma.cc/5RJH-9VWZ].

[43] Yves Barlette et al., *Bring Your Own Device (BYOD) as Reversed IT Adoption: Insights into Managers' Coping Strategies*, 56 INT'L. J. INFO MGMT. (2021).

[44] BEYOND IDENTITY, *supra* note 37.

[45] MORPHISEC, 2021 WFH EMPLOYEE CYBERSECURITY THREAT INDEX (2021) at 5.

[46] Diane Garey, *BYOD and Mobile Security: 2016 Spotlight Report Results*, TENABLE (Apr. 5, 2016), https://www.tenable.com/blog/byod-and-mobile-security-2016-spotlight-report-results [https://perma.cc/VM8E-6VFP].

[47] SAMSUNG, MAXIMIZING MOBILE VALUE: IS BYOD HOLDING YOU BACK?, OXFORD ECONOMICS (June 2018) at 3.

In addition to the increasing use of personal devices for work, another concerning trend is the rising use of work devices for personal matters and the general commingling of personal and employment-related uses across devices. One survey from 2022 suggested that 50% of adults use employer-issued devices to check personal email and messages, while 45% read news, 32% shop online, and 28% view social media.[48] Beyond Identity's 2021 survey broke down personal activities into more categories with slightly differing results, finding that roughly a third of employees had used work-issued devices to send or check personal emails, with slightly fewer having shopped online.[49] Roughly a quarter of employees had accessed social media or streamed videos or music, while roughly 20% had conducted bank or financial transactions.[50] A smaller number of employees had engaged in even more questionable activities, with roughly 10% of in-person employees having viewed adult or pirated content on work-issued devices.[51] An earlier 2020 survey conducted by the cybersecurity company Malwarebytes Labs that surveyed primarily remote workers similarly found that 52.6% of surveyed employees had sent or received personal emails, while 52% had checked the news, 37.8% had shopped online, and 25% had checked social media.[52] For employees who refrain from using employer-issued devices for personal purposes, studies suggest that they often use their mobile phones for those purposes, the same personal phones that are increasingly integral to work as well.[53] Again, while statistics are limited and unreliable, the available data suggests that there is increasing commingling of work and personal activities on the same devices – while personal activities on work devices might once have been limited to relatively innocent web browsing, employees are now increasing conducting activities like shopping and accessing personal financial information on devices used for work, potentially exposing their financial information to their employers.

---

[48] Ani Petrosyan, *Adults Worldwide Using Employer-Issued Devices for Personal Activities in 2022, by Activity*, STATISTA (last accessed Oct. 10, 2023), https://www.statista.com/statistics/1147849/share-adults-worldwide-employer-issued-device-personal-activities/#statisticContainer.

[49] BEYOND IDENTITY, *supra* note 37.

[50] *Id.*

[51] *Id.*

[52] Phillip Christian, *Risky Business: Survey Shows Majority of People Use Work Devices for Personal Use*, MALWAREBYTES LABS (Oct. 7, 2020), https://www.malwarebytes.com/blog/news/2020/10/work-devices-for-personal-use [https://perma.cc/8UHS-TCJG].

[53] *See, e.g.*, Dock Treece, *How Much Time are Your Employees Wasting on Their Phones?*, BUS. NEWS DAILY (Feb. 21, 2023), https://www.businessnewsdaily.com/10102-mobile-device-employee-distraction.html [https://perma.cc/L4CT-SDVK]; Jonathan Berr, *Your Smartphone is Making You a Workplace Slacker*, CBS NEWS (June 9, 2016), https://www.cbsnews.com/news/your-smartphone-is-making-you-a-workplace-slacker/ [https://perma.cc/54NQ-2YX8].

Employers are quite aware of this sloppy, mixed use of devices. Indeed, employers have been trying to ensure work-focused use of devices for decades, and at this point, many if not most employers have policies that regulate proper use of devices.[54] Often termed "appropriate use" policies, these documents set ground rules for permissible and impermissible uses and conduct on employer devices and networks and are often complemented by BYOD policies, which aim to delineate permissible conduct on BYOD devices.[55]

Employers seem to lack the means to adequately enforce device use policies, or perhaps so many employees flout them that enforcement is simply unfeasible. Regardless of the cause, employees continue to use the same devices both for work and for personal matters. Anecdotally, it makes sense that this trend would be rising contemporaneously with the increase in remote work – as employees increasingly work in the same places that they live, without the temporal and geographic separation created by "clocking in" at a physical office for a set number of hours, it seems logical that they would intersperse the personal with the professional in their use of devices, particularly when employers often require them to use their own personal devices for work.

Since the Covid-19 pandemic and the accompanying rise in remote work, many companies have become increasingly concerned with employees engaging in personal activities during work time, developing a "productivity paranoia" in which businesses seek to respond to a perceived lack of focus amongst remote employees. Some employers have gone a step further than mere device use policies, instead actively monitoring employee use of devices through surveillance programs.[56] But device use policies and even active monitoring

[54] GARRY G. MATHIASON ET AL., *THE "BRING YOUR OWN DEVICE" TO WORK MOVEMENT: ENGINEERING PRACTICAL EMPLOYMENT AND LABOR LAW COMPLIANCE SOLUTIONS, LITTLER* (2012), https://www.littler.com/files/press/pdf/TheLittlerReport-TheBringYourOwnDeviceToWorkMovement.pdf.

[55] For typical template examples of acceptable use and BYOD policies, *see, e.g.*, Lawson Lundell, *Sample Employer Policy – Acceptable Use Policy*, https://www.lawsonlundell.com/assets/htmldocuments/Sample%20Acceptable%20Use%20Policy%20January%202020.pdf (last visited Jan. 10, 2024); *Bring Your Own Device (BYOD) Policy*, SHRM, https://www.shrm.org/topics-tools/tools/policies/bringyourowndevicepolicy [https://perma.cc/BU2P-SADR] (last visited Jan. 10, 2024).

[56] *See, e.g.*, *How Much Employee Monitoring is too Much?*, AMERICAN BAR ASSOCIATION (Jan. 2018), https://www.americanbar.org/news/abanews/publications/youraba/2018/january-2018/how-much-employee-monitoring-is-too-much-/ [https://perma.cc/T38B-WEG7]; Goh Chiew Tong, *Employee*

appear to have limited effect – employees seem to have become inured to the idea of employer monitoring and simply do not care, continuing to engage in personal activities or even taking more personal time in retaliation for suspected monitoring.[57] Indeed, some surveys suggest that increasing employer pressure to be productive results in "productivity theater," causing employees to act in ways that feign productivity, such as excessive meetings and emails, while perhaps reducing the amount of actual work accomplished.[58]

C. Instrumentalities Enabling Remote Access

Having examined the growing prevalence of remote work, the increasing use of personal devices, and the increasingly commingled use of the same devices for both work and sensitive personal matters, a particularly important question for this paper is how exactly employees are creating remote access for employees: what systems are being but in place to allow employees to remotely access employer files, servers, and programs, and to what extent do these remote access systems give employers (and potentially malicious hackers) a window into employee activity and data? This section of the paper will discuss the two most common systems of enabling remote access – VPNs and cloud providers – and how those systems give an employer a window into an employee's activities. Lastly, outside of the instrumentalities by which remote access is provided, this section will discuss other programs that employers might utilize that could, intentionally or otherwise, create an opening to view activity on employee devices.

Surveillance is on the Rise — and That Could Backfire on Employers, CNBC (Apr. 23, 2023), https://www.cnbc.com/2023/04/24/employee-surveillance-is-on-the-rise-that-could-backfire-on-employers.html [https://perma.cc/D5LX-FMN3].

[57] *See, e.g.*, Paresh Dave, *Employees assume bosses track their work computers, survey finds*, L.A. TIMES (May 23, 2013), https://www.latimes.com/business/technology/la-fi-tn-employees-computer-monitoring-20130522-story.html [https://perma.cc/Y5BH-T64B]; Chase Thiel et al., *Monitoring Employees Makes Them More Likely to Break Rules*, HARV. BUS. REV. (June 27, 2022), https://hbr.org/2022/06/monitoring-employees-makes-them-more-likely-to-break-rules [https://perma.cc/CV99-2JEH].

[58] Microsoft, *Hybrid Work Is Just Work. Are We Doing it Wrong?* (Sept. 22, 2022), https://www.microsoft.com/en-us/worklab/work-trend-index/hybrid-work-is-just-work [https://perma.cc/ZU6V-5MFJ]; Jessica Stillman, *Remote Workers are Wasting More Than an Hour a Day on Productivity Theater, New Report Finds*, INC. (Aug. 22, 2022), https://www.inc.com/jessica-stillman/productivity-asynchronous-remote-work.html [https://perma.cc/2FAR-SDU7].

1. VPNs

VPNs, or virtual private networks, are a tool used to establish a protected network connection, disguising the online identity of a device to third parties.[59] In a remote work arrangement, this would be accomplished by having the employer create a specially configured remote server, the VPN host. Employees seeking to connect to employer files would connect first to the VPN, and then through the VPN access files and programs on the employer's actual servers as well as navigating the internet through the VPN. Passing all traffic through the VPN provides the opportunity to encrypt traffic with the employer's home server and also means that the employee's IP address can be hidden, as can the employee's geographic location.

VPNs are simple and powerful arrangements that can create a secure, reliable connection with employees. However, while the encryption of VPNs makes traffic through the VPN harder for third parties to access from outside the system, it means that the employer controls any traffic that passes through the VPN, including anything that the employee does online while connected to the VPN. This level of access could be highly granular – any traffic, down to individual keystrokes, that passes through the VPN could theoretically be visible, if the owner of the VPN were to put in place software that enabled monitoring of that traffic.[60] In practice, very few if any employers appear to actually utilize their control over the VPN to surveil employee web traffic, and beyond a select group of network administrators and IT specialists, the management of many employers may not be aware that the VPN presents this opportunity. However, the ability to utilize this control creates the possibility that a malicious actor who gained access to and control over the employer's systems could use the VPN from the inside, viewing employee activity on the VPN and harvesting valuable and sensitive personal information gleaned from employee web traffic.[61]

---

[59] For a basic summary of the function of a VPN, *see generally* Mark Smirniotis, *What Is a VPN and What Can (and Can't) It Do?*, N.Y. TIMES (Mar. 3, 2021) https://www.nytimes.com/wirecutter/guides/what-is-a-vpn/ [https://perma.cc/72WD-NZT3].

[60] For an example of software providers in the marketplace today offering tools that enable some level of VPN monitoring, *see, e.g.*, THOUSAND EYES, *VPN Monitoring*, https://www.thousandeyes.com/solutions/vpn-monitoring [https://perma.cc/4GYL-WC8X] (last visited Jan. 10, 2024); Doug Barney, *What is VPN Monitoring?*, PROGRESS WHATSUP GOLD (Oct. 26, 2021), https://www.whatsupgold.com/blog/what-is-vpn-monitoring [https://perma.cc/49R5-MSFQ].

[61] Tong, *supra* note 56.

2. Cloud-Based Systems

While VPNs offer security and significant customizability, some employers chose the more turnkey solution presented by cloud services – as it is used in the world of remote access, this term refers to solutions that turn to a third party to host data or applications on the "cloud," which employees then access by connecting to the third-party system through a web-based interface.[62] Cloud-based systems can range in complexity from a full remote desktop to more minimal cloud-based hosting of files or specific applications.[63] And a cloud-based system may also involve a VPN –but a VPN hosted by the third-party providing the cloud services, rather than the employer.[64]

By contracting with a cloud-based third party to provide remote access, an employer can avoid the ongoing burden of monitoring and security, instead relying on a much larger, technically specialized cloud provider such as Microsoft, Google, or Amazon to ensure that security is up to date and that remote access systems do not fail.[65] On the other hand, the employer loses control over security, and is reliant on a third party – if the third party's systems are breached, the employer will have less control over the incident and may take longer to find out. At the same time, the company also loses its window into employee activities. As it does not control the servers that employee activity passes through, it can no longer view activity on such a granular level (though some data such as websites accessed, programs used, or files viewed through a remote desktop may still be visible).

3. Applications Enabling Employer Access and Surveillance

Apart from the window that employers may have into employee activities through the remote access protocol used by a company, employers are able to use other programs installed on employee devices to create a window that allows them to view an employee's activity. Such programs can be intended purely for benign purposes – one of the most

---

[62] For a discussion of the basics of cloud computing and different cloud service models, *see generally* Nadia Reckmann, *Cloud Computing: A Small Business Guide*, Business News Daily (Dec. 20, 2023), https://www.businessnewsdaily.com/4427-cloud-computing-small-business.html [https://perma.cc/9LTK-9YAH].

[63] *Id.*

[64] Andrew Froehlich *How Do VPN vs. Cloud Services compare for Remote Work?,* TECH TARGET (Nov. 11, 2020), https://www.techtarget.com/searchnetworking/answer/How-do-VPN-vs-cloud-services-compare-for-remote-work [https://perma.cc/PQ9Q-9L6T].

[65] *See, e.g.*, AMAZON WEB SERVS., *AWS Remote Work Solutions*, https://aws.amazon.com/remote-work-learning/ [https://perma.cc/A5RS-4M6T] (last visited Jan. 10, 2024).

common such programs is "TeamViewer" and other similar remote control programs, which allows a user to remotely access another computer, taking over of the mouse and gaining control of the accessed machine.[66] This line of programs was created in large part to allow IT specialists to remotely access employee devices for maintenance and troubleshooting, though of course they potentially could be misused to access employee devices for malicious purposes by hackers who were able to access and control employer systems.[67] In practice, remote access programs that allow active control generally display a notification on the accessed computer when access has been created and allow an individual physically present at that computer to terminate access, limiting potential misuse.[68] Some maintenance programs, however, are designed to operate in the background, allowing IT professionals to push updates to employee devices and install new applications as employers roll out new initiatives.[69]

Other remote monitoring programs are intended to enable not mere maintenance or support, but actual surveillance of employees. In a perhaps misguided effort to encourage productivity in the workforce, some employers have turned to programs intended to track and monitor employee activities.[70] Some of these "productivity" applications monitor web traffic, notifying employers of what websites employees access, how much time employees spend there, and whether they stream media.[71] Others can monitor work applications, assessing how much time employees take in responding to emails, editing word documents, and completing assigned tasks. And others may provide even more comprehensive

[66] *See generally, id.*

[67] For one account of a remote access attack in practice, *see generally* Jason Knowles & Ann Pistone, *Hackers Use Remote Access Trojan, or RAT, Attacks to Force Way into Computer, Access Accounts*, ABC7 (Feb 29, 2024), https://abc7chicago.com/remote-access-trojan-horse-virus-rat-attack-computer-hacking/14479523/ [https://perma.cc/C5C9-PZCT].

[68] *Id.*

[69] For a discussion of remote patch management programs and similar remote maintenance tools, *see generally* Robert Sheldon, *12 Best Patch Management Software and Tools for 2024*, TECHTARGET (Dec. 1, 2023), https://www.techtarget.com/searchenterprisedesktop/tip/12-best-patch-management-software-and-tools [https://perma.cc/4SRX-6G2Q].

[70] For a discussion of the prevalence of employer surveillance tools and the types of programs commonly used, *see generally*, CurrentWare, *Real-Time Employee Monitoring Software for Workforce Productivity*, https://www.currentware.com/products/browsereporter/?gclid=Cj0KCQiAmNeqBhD4ARIsADsYfTeNWG7OWod3xS0XBBOh_LOLo9X6HyVSXZFawi6fcouoKcqaHlq1LVEaAi6VEALw_wcB [https://perma.cc/7ADM-ZKZM] (last visited Nov. 16, 2023); Wakefield Research, *2023 Employee Productivity Surveillance Technology Survey* (2023), https://www.1e.com/resources/report/employee-surveillance-technology-survey/.

[71] *See* CurrentWare, *supra* n. 70.

surveillance, such as keyloggers[72] that record every key pressed by an employee and screen capture software[73] that actively records an employee's screen over an extended period. These programs provide employers with exceptionally powerful tools to monitor employees. However, if a malicious outsider was able to access and control employer systems, they could easily misuse these types of programs to gain access to sensitive information about employees, particularly where employees used work devices for personal activities as well.

II. DATA BREACHES

A. Taxonomy of Data Breaches

Since the invention of the internet, individuals and groups often referred to as "hackers" have sought to push the limits of unauthorized access, taking advantage of technological tools, psychological tactics, and user error to gain access to private and state computer systems. Hackers have historically had a variety of motivations, including international espionage and the sheer allure of a challenge, yet increasingly cybercrime has come to be dominated by actors seeking monetary gain, who have gone after targets possessing repositories of data perceived to be valuable.[74]

The first major data breaches involving sensitive consumer information occurred in the early 2000s, with attacks against retailers such as TJX Companies[75] (the owner of T.J. Maxx and Marshalls) and DSW Shoe Warehouse.[76] In the early 2010s, a spate of major cyberattacks directed against companies that held significant amounts of credit card data brought the issue into the public eye. In December 2013, Target reported a breach of its customer data files that exposed information of more than 40 million customers in what

[72] *See, e.g., Keylogger Software for Monitoring and Recording Keystrokes*, EKRAN https://www.ekransystem.com/en/product/employee-keylogging [https://perma.cc/4B35-QN9T] (last visited Nov. 16, 2023).

[73] *See, e.g.*, *Screen Video Recording*, KICKIDLER https://www.kickidler.com/video-recording.html [https://perma.cc/WMZ6-2G9H] (last visited Nov. 16, 2023).

[74] *See, e.g.*, Jack Denton, *How Ransomware Gangs Are Fueling a New Cybersecurity Arms Race*, BARRONS (Dec. 6, 2023), https://www.barrons.com/articles/ransomware-gangs-cybercrime-cybersecurity-crypto-09d5318c. [https://perma.cc/V44S-RW6J]

[75] Kim Zetter, *TJX Failed to Notice Thieves Moving 80-GBytes of Data on its Network*, WIRED (Oct. 26, 2007), https://www.wired.com/2007/10/tjx-failed-to-n/ [https://perma.cc/477P-QB4E].

[76] Federal Trade Comm'n, *DSW Inc. Settles FTC Charges,* FTC (Dec. 1, 2005), https://www.ftc.gov/news-events/news/press-releases/2005/12/dsw-inc-settles-ftc-charges [https://perma.cc/NCX2-F8FR].

remains one of the largest data breaches in history.[77] The breach exposed credit and debit accounts as well as non-financial personal information including names, phone numbers, and email addresses that left up to 70 million customers vulnerable to identity theft.[78] In the same year, a data breach at Yahoo exposed 3 billion user accounts and all of the information that they contained.[79] In 2014, Home Depot suffered a similar breach that exposed the payment card data of roughly 40 million customers,[80] while eBay[81] and JP Morgan Chase,[82] also suffered significant data breaches that exposed account information of tens, if not hundreds of millions of customers. As if these attacks hadn't been sufficient to put businesses, the public, and the legal system on notice to the threat of data breaches, the next year brought a series of data breaches at the Federal Office of Personnel Management that exposed the personnel files of 4.2 current and former government employees, the security clearance background investigation information of 21.5 million individuals, and fingerprint data for 5.6 million individuals.[83] The OPM breach illustrated that no company or entity was immune to data breaches, no matter how sophisticated they might be, and even the federal government was vulnerable to

[77] *See, e.g.*, Kevin McCoy, *Target to Pay $18.5M for 2013 Data Breach that Affected 41 Million Consumers*, USA TODAY (May 23, 2017), https://www.usatoday.com/story/money/2017/05/23/target-pay-185m-2013-data-breach-affected-consumers/102063932/ [https://perma.cc/TJ8F-2U9N]; MAJORITY STAFF OF S. COMM. ON COMMERCE, SCI., AND TRANSP., *A "Kill Chain Analysis of the 2013 Target Data Breach* (Mar. 26, 2014), https://www.commerce.senate.gov/services/files/24d3c229-4f2f-405d-b8db-a3a67f183883 [https://perma.cc/7LKN-5FHM].

[78] MAJORITY STAFF OF S. COMM. ON COMMERCE, SCI., AND TRANSP., *supra* note 77.

[79] Nicole Perlroth, *All 3 Billion Yahoo Accounts were Affected by 2013 Attack*, N.Y. TIMES (Oct. 3, 2017), https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html [https://perma.cc/XZ5K-GJ6A]

[80] Jonathan Stempel, *Home Depot reaches $17.5 million settlement over 2014 data breach*, REUTERS (Nov. 24, 2020), https://www.reuters.com/article/us-home-depot-cyber-settlement/home-depot-reaches-17-5-million-settlement-over-2014-data-breach-idUSKBN2842W5 [https://perma.cc/GH7Y-PSJ5].

[81] *Hackers raid eBay in historic breach, access 145M records*, CNBC (May 22, 2014), https://www.cnbc.com/2014/05/22/hackers-raid-ebay-in-historic-breach-access-145-mln-records.html [https://perma.cc/HT49-KUT4].

[82] Jessica Silver-Greenberg et al., *JPMorgan Chase Hacking Affects 76 Million Households*, N.Y. TIMES (Oct. 2, 2014), https://archive.nytimes.com/dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/ [https://perma.cc/24AK-H8UK].

[83] STAFF OF H.R. ON OVERSIGHT AND GOVERNMENT REFORM, 114TH CONG., THE OPM DATA BREACH: HOW GOVERNMENT JEOPARDIZED OUR NATIONAL SECURITY FOR MORE THAN A GENERATION (Sept. 7, 2016).

determined hackers. In the wake of the OPM breach, congressional oversight led to a new wave of federal and state legislation targeting cybercrime.[84]

Most of these early data breaches involved the exposure of information, either in one short-term event or through a longer-term intrusion into a protected system. In these types of data breaches, the focus of the hackers is immediate, one-time access to data, which has value when extracted from the target system and either used directly by the criminals themselves or sold on to other parties.[85]

As cybercrime evolved, some hackers turned to a novel form of attack that sought to monetize not specific stolen data, but persistent access to a private network. Termed a "ransomware" attack, these hackers use their access to install their own malware that locks out the legitimate users of the platform until a ransom is paid.[86] While the first successful ransomware attacks appeared in the early 2000s, the tactic took over when the increasing viability of bitcoin and blockchain transactions made it easier for would-be ransomers to obtain payment without giving away their location or identity to the victim.[87] First appearing in 2011, the Gameover Zeus scam was a prominent early example of a bitcoin-reliant ransomware scheme, with a criminal organization using phishing and social engineering schemes to create a substantial "botnet"[88] which was then used to deliver CryptoLocker, a ransomware program that locked out users from infected devices and demanded a payment in bitcoin in order to decrypt and recover files.[89]

---

[84] *See infra* Section B(ii) for a discussion of state and federal statutes passed in the wake of the OPM breach.

[85] *What is a Data Breach?*, IBM https://www.ibm.com/topics/data-breach [https://perma.cc/C4US-PTDL] (last visited Mar. 24, 2024)

[86] *What is Ransomware?*, IBM https://www.ibm.com/topics/ransomware [https://perma.cc/W58F-3UU8] (last visited Mar. 24, 2024)

[87] *See* Denton, *supra* note 74.

[88] A botnet is a network of internet-connected devices, each of which has been infected with malware (malicious software) that allows it to be remotely controlled by a third party. This malicious third-party actor can then use all devices in the botnet for purposes such as phishing, distribution of malware, or in unison to conduct a DDOS (distributed denial of service) attack. Katie Terrell Hanna, *Botnet*, TECHTARGET (Mar. 6, 2021), https://www.techtarget.com/searchsecurity/definition/botnet [https://perma.cc/Y98F-7H3U].

[89] *E.g.*, U.S. Dept. of Justice, *U.S. Leads Multi-National Action Against "Gameover Zeus" Botnet and "Cryptolocker" Ransomware, Charges Botnet Administrator* (June 2, 2014); Bryan Prince, *Gameover Zeus, CryptoLocker Hit in Massive Takedown Operation*, SECURITY WEEK (June 2, 2014), https://www.securityweek.com/gameover-zeus-cryptolocker-hit-massive-takedown-operation/ [https://perma.cc/WS68-89FR].

CryptoLocker is estimated to have infected as many as 250,000 systems worldwide, and total ransoms collected through the malware may have totaled tens of millions of dollars before the scheme was shut down.[90] Since the early 2010s, the technical capabilities and pace of ransomware attacks have only increased, and costs have grown as well. Assessing the full scope of ransomware attacks is difficult as businesses often do not report attacks, but a 2013 report by cybersecurity consultancy Cybersecurity Ventures estimated total ransomware damages of $325 million worldwide in 2013, an amount that was estimated to reach as much as $20 billion in 2021.[91] A recent report by IBM indicated that the average ransomware attack globally now costs the target as much as $4.45 million, an amount that had increased from $3.62 million in 2017.[92] In the US, average costs of data breaches were the highest in the world, reaching $9.48 million in 2023.[93]

Over the ten years since the CryptoLocker attacks, ransomware attackers have refined their tactics. Early organizations like the malicious actors behind CryptoLocker focused on deriving value from locking down access to the target's data and forcing the target to pay money to restore access, a so-called "data kidnapping" or classic ransomware.[94] But rather than threaten to lock the user out, other malicious actors have used ransomware to threaten to publish the hacked data unless the user pays a ransom, a type of attack termed "extortionware," "leakware" or "doxxware[.]"[95] This evolution permits criminals to derive extra value from businesses whose data may not have significant intrinsic value if

---

[90] *E.g.*, Chris Brook, *CryptoLocker Creators Infected Nearly 250,000 Systems, Earned $300k Since September*, THREATPOST (Dec. 30, 2014), https://threatpost.com/cryptolocker-creators-infected-nearly-250000-systems-earned-30m-since-september/103261/ [https://perma.cc/7JAZ-6Y6L]; Dan Goodin, *You're infected—if you want to see your Data Again, Pay Us $300 in Bitcoins*, ARS TECHNICA (Oct. 17, 2013), https://arstechnica.com/information-technology/2013/10/youre-infected-if-you-want-to-see-your-data-again-pay-us-300-in-bitcoins/ [https://perma.cc/V2L6-QTDT].

[91] Steve Morgan, *Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031*, CYBERCRIME MAGAZINE (Jul. 7, 2023), https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/ [https://perma.cc/5K5E-K6UC].

[92] IBM SECURITY, COST OF A DATA BREACH REPORT 2023 (2023).

[93] *Id.*

[94] Kurt Baker, *History OF Ransomware*, CROWDSTRIKE (Oct. 10, 2022), https://www.crowdstrike.com/cybersecurity-101/ransomware/history-of-ransomware/ [https://perma.cc/5D9Q-ZWVZ].

[95] *See, e.g.*, Rob Shavell, *Extortionware Is on the Rise. Here's How to Anticipate and Prevent Attacks Before They Happen*, CORPORATE COMPLIANCE INSIGHTS (May 25, 2021), https://www.corporatecomplianceinsights.com/extortionware-prevent-attacks-cybersecurity-threat/ [https://perma.cc/2PNC-H2ZA].

sold on the web, but whose business models or functions make them vulnerable to significant reputational costs if their data were to be exposed.

At the same time, malicious actors have advanced in their methods for target selection and the spread of their ransomware. Early attacks like CryptoLocker used tactics like botnets to simply spread their malware to as many users as possible and tried to extract small sums of money from a substantial number of affected parties, many of whom were ordinary individuals without significant resources.[96] More recently, ransomware attacks have focused on so-called "big-game hunting," using phishing and social engineering to seek an entry point to the systems of well-researched entities perceived as high-value targets.[97] As part of this shift, ransomware attackers have expanded beyond their initial focus in the private sector to target the public sector, with successful ransomware attacks on numerous government entities ranging from the Illinois Attorney General's Office to the City of Dallas and the U.S. Department of Energy, to name a few.[98] In total, one commentator estimated that roughly 330 ransomware attacks were conducted against government institutions between 2018 and October 2022, costing over $70 billion.[99]

In sum, over the last decade, the threat of data breaches has grown exponentially. Businesses, individuals, and governments have all attempted to address the threat, and many entities have made improvements in data security–IBM's 2023 study of the costs of data breaches found that factors such as security system complexity, the presence of sufficient staff with security skills, and employee training all reduced the average costs of

[96] Baker, *supra* note 94.

[97] *See, e.g.*, David Carlisle, *Ransomware & Crypto: The Growing Compliance Challenge*, REUTERS (May 1, 2023), https://www.reuters.com/legal/legalindustry/ransomware-crypto-growing-compliance-challenge-2023-05-01/ [https://perma.cc/89B3-H8QG].

[98] Jared Rutecki & Ray Long, *No Ransom Paid, But Hacker Attack Costs Illinois AG Office More than $2.5 million, Says Kwame Raoul*, CHICAGO TRIBUNE (Jul. 29, 2021), https://www.chicagotribune.com/investigations/ct-ransomware-attack-illinois-attorney-general-kwame-raoul-20210729-diukhbzjanhgzlcntft3nakbfy-story.html [https://perma.cc/54TR-LFL4]; Sean Lyngaas, *Exclusive: US government agencies hit in global cyberattack*, CNN (June 15, 2023), https://www.cnn.com/2023/06/15/politics/us-government-hit-cybeattack/index.html [https://perma.cc/P65S-HG29]; Sam Sabin, *Ransomware gangs zero in on under-resourced U.S. cities and towns*, AXIOS (May 16, 2023), https://www.axios.com/2023/05/16/ransomware-us-cities-towns-local-government-hackers [https://perma.cc/LKZ8-6CN7].

[99] Paul Bischoff, *Ransomware attacks on US government organizations cost over $70bn from 2018 to October 2022*, COMPARITECH (Nov. 9, 2022), https://www.comparitech.com/blog/information-security/government-ransomware-attacks/ [https://perma.cc/6EZD-WM2U].

data breaches substantially.[100] However, for each organization that proactively adopts security systems and trains employees, there are others with exacerbating factors such as a remote workforce, cloud-based computing, employer surveillance, a shortage of security skills, and noncompliance with regulations, all of which increase vulnerabilities and the likely costs of data breaches.[101] Mere technical sophistication is no longer sufficient to ward of cyberattacks, which increasingly rely on stolen credentials, malicious insiders, phishing, and social engineering–even the most elaborate network security cannot guard against human foibles.[102] The arms race between malicious hackers and network administrators will continue, but for now everyone should consider their systems vulnerable to breach.

B. Evolution of Data Breach Law

Data breach law is a body of case law and statutes that has developed rapidly over the past quarter century in the face of a rapidly proliferating data breaches of increasing scale. While the earliest consumer cases involving data breaches focused on largely on common law claims, new state and federal statutes as well as more case law clarifying issues of liability have sharpened the tools available to private lawsuits. State and federal enforcement actions have evolved as well. While early enforcement cases against companies that had suffered data breaches often focused on general authority to prosecute deceptive and unfair conduct in the marketplace under broad statutes such as the Federal Trade Commission Act (FTC Act), Dodd-Frank Act, and Fair Credit Reporting Act (FCRA), new legislation has created affirmative responsibilities for businesses specific to data breaches. In addition to federal action, many states have stepped in to fill the vacuum created by a slow-moving congress, creating a patchwork of data security laws across the country. This section will examine the types of claims, common law and statutory, brought by plaintiffs in data breach cases, particularly those arising out of an employment context. Examining common stumbling blocks and key factors asserting for successful claims, the section will contrast these private claims with data breach enforcement actions brought by state and federal regulators.

[100] IBM SECURITY, COST OF A DATA BREACH REPORT 2023 at 16–17 (2023).
[101] *Id.*
[102] *Id.* at 21.

1. Common Law Claims

Issues of standing, duty, and damages dominated discussions of early attempts to bring common law claims for data breaches. Consumers and employees have attempted to rely upon a range of different common law claims with mixed results.[103]

a. Tort Claims

Many successful complaints have sought to recover damages for a data breach based on a claim of negligence, alleging that businesses owe customers or employees a duty to exercise reasonable care in collecting and storing data.[104] Other plaintiffs have successfully alleged negligent misrepresentation, arguing that companies misrepresented their data protection policies to individual users.[105] And other parties have brought successful contract claims, alleging that companies breached an express or implied contract with employees or users when they failed to keep data safe.[106]

Other claims have been attempted, but with less consistent success. Some plaintiffs have gone a step further than negligence, arguing that the interaction between an individual and a company might give rise to a fiduciary relationship that imposed higher duties on the company to safeguard data, though some courts have rejected arguments for finding a fiduciary relationship between employers and employees for data security.[107] Other

---

[103] For more discussion of particular claims, *see generally Liability of Employer for Breach of Data Security for Employee Information*, 87 A.L.R. 7th Art. 1 (2023); Monique C.M. Leahy, *Litigation of Data Breach*, 140 AM. JUR. TRIALS 327 (2023).

[104] *E.g.*, Clemens v. ExecuPharm Inc., 48 F.4th 146 (3d Cir. 2022) (where data breach exposed employee data, court held employee has sufficiently alleged injury in fact to bring claim for negligence); Ramirez v. Paradise Shops, LLC, 69 F.4th 1213 (11th Cir. 2023) (employee has standing to bring negligence claim based on data breach that exposed personal employee data).

[105] *Clemens*, 48 F. 4th 145.

[106] *Id.* (holding that employees had sufficiently alleged breach of express provision stemming from data breach where company had contracted to "take appropriate measures to protect the confidentiality and security" of employee data); Castillo v. Seagate Technology, LLC, No. 16-cv-01958-RS, 2016 WL 9280242 (N.D. Cal. 2016) (employees sufficiently alleged brief of implied contact where employer released W-2 tax forms in data breach).

[107] In re Waste Management Data Breach Litigation, Nos. 21cv6147, 21cv6199, 21cv6257, 21cv6902, 2022 WL 561734 (S.D.N.Y. 2022) (rejecting argument that employers have fiduciary duty to employees to safeguard data, even where company required employees to share personal information). *But see*, *e.g.*, *Clemens*, 48 F. 4th 145 (holding employee had standing to bring breach of fiduciary duty claim against employer for data breach).

plaintiffs have tried to bring claims for invasion of the right to privacy or similar "breach of confidence" torts, though these have often been rejected by courts, which have noted that these claims require a showing that an employer improperly obtained personal information, intentionally disclosed it to third parties, or placed the information in the public view, beyond mere disclosure.[108] Similarly, asserting claims for unjust enrichment has proven to be difficult in a data breach context, and plaintiffs have failed more often that they have succeeded – successful unjust enrichment claims based on a data breach have alleged that a company received a benefit from the injured parties, was enriched at their expense when it chose to cut costs by not implementing security measures, and that it would be inequitable for the company to retain the money saved by shirking data security.[109]

b. Contract Claims

Outside of tort claims and unjust enrichment, many plaintiffs have sought to bring contractual claims against companies arising out of data breaches. Here, success can vary depending on what contractual provisions a plaintiff can point to. In *Clemens v. ExecuPharm*, for example, where a company had contracted with employees to "take appropriate measures to protect the confidentiality and security" of the sensitive personal information of its employees, that provision was found to be sufficient to support a claim of breach after a data leak.[110] Beyond explicit contractual provisions, some cases have sought to rely on general contractual principles such as covenants of good faith and fair dealing – depending on state law, some plaintiffs have succeeded in asserting these claims, but results have been mixed.[111]

---

[108] *E.g.*, Elliott-Lewis v. Laboratories, 378 F. Supp. 3d 67 (D. Mass. 2019) (finding that invasion of privacy under MA law requires showing of intent and dismissing claim based on data breach); McKenzie v. Allconnect, Inc., 369 F. Supp. 3d 810 (E.D. Ky. 2019) (finding that data breach did not give rise to claim for invasion of privacy based on publicity as data breach did not constitute "publication" under KY law).

[109] *E.g.*, Sackin v. TransPerfect Global, Inc., 278 F. Supp. 3d 739 (S.D.N.Y. 2017) (finding complaint adequately alleged unjust enrichment). *But see, e.g.*, Linman v. Marten Transport, Ltd., No. 22-cv-204-jdp, 2023 WL 2562712 (W.D. Wis. 2023) (rejecting unjust enrichment claim where plaintiff identified no benefit that his personal information provided to defendant company).

[110] 48 F. 4th at 156.

[111] *Compare* Mackey v. Belden, Inc., No. 4:21-CV-00149-JAR, 2021 WL 3363174 (E.D. Mo. 2021) (finding that Missouri law implied covenant of good faith and that employee had plausibly alleged breach) *with* Reetz v. Advocate Aurora Health, Inc., 983 N.W.2d 669 (Wis. Ct. App. 2022) (finding that Wisconsin law required a valid contract with express terms for a claim of breach of the covenant of fair dealing, and plaintiffs had not shown contract requiring protection of data).

More importantly, even in the absence of explicit contractual provisions or traditional contract principles, numerous courts have permitted claims based on an implied breach of contract, especially in the context of employment relationships.[112] *Castillo v. Seagate Tech.*, an early case permitting a claim for implied breach of contract based on data breach, sums up the logic behind such a claim and provides a sobering message for employers.[113] In *Castillo*, employees of Seagate Technology brought claims against their employer after a 2016 incident in which the company inadvertently released W-2 data for all employees in a phishing scheme.[114] Among other claims, the employees alleged a breach of an implied contract, arguing that they had provided their data to Seagate to receive employment and benefits with the understanding that Seagate would "take adequate measures to protect it."[115] Seagate argued that the plaintiffs had shown no conduct evincing mutual understanding or assent to this supposed agreement and that the plaintiffs had failed to specify the scope of the supposed protection that their data was to be afforded, but the court found these arguments to be unavailing, stating that "it is difficult to imagine how, in our day and age of data and identity theft, the mandatory receipt of Social Security numbers or other sensitive personal information would not imply the recipient's assent to protect the information sufficiently."[116]

Rejecting Seagate's argument that the plaintiffs should have asserted a specific form of protection that the parties agreed to, the court found that the plaintiffs' assertion of a general understanding that adequate security measures would be employed represented "a far more realistic reflection of the mutual agreement that occurs in most data-sharing

[112] *E.g.*, In re Arthur J. Gallagher Data Breach Litigation, No. 22-cv-137, 2022 WL 4535092 (N.D. Ill. 2022) (finding that company privacy policy representing that company would restrict access to employee data to those who required access for "legitimate, relevant business purposes" supported finding an implicit promise to protect employee personal information in exchange for employment); McKenzie v. Allconnect, Inc., 369 F. Supp. 3d 810 (E.D. Ky. 2019) (finding that to assert a claim for breach of implied contract, it was sufficient to allege that employees were required to provide personal information as a condition of employment, and that employer implicitly agreed to safeguard that information); Mackey v. Belden, Inc., No. 21-CV-149, 2021 WL 3363174 (E.D. Mo. 2021) (citing other cases for proposition that "it is difficult to imagine how, in our day and age of data and identity theft, the mandatory receipt of … sensitive personal information would not imply the recipient's assent to [sic] the protect the information sufficiently.") (quoting Castillo v. Seagate Tech., LLC, No. 16-CV-01958, 2016 WL 9280242, at *9 (N.D. Cal. Sept. 14, 2016).

[113] 2016 WL 9280242 at *9.

[114] *Id.* at *1.

[115] *Id.* at *9.

[116] *Id.*

transactions: When a person hands over sensitive information, in addition to receiving a job, good, or service, they presumably expect to receive an implicit assurance that the information will be protected."[117] Subsequently, federal and state courts around the country have cited *Castillo* in finding an implied understanding that reasonable measures will be used to protect data.[118]

c. Standing, Damages, and Causation in Data Breach Cases

Across all these claims, one common threshold question is whether plaintiffs have standing to assert a claim based on a data breach. To establish Article III standing, plaintiffs must allege that they have "(1) suffered an 'injury in fact' that is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical; (2) the injury is fairly traceable to the challenged action of the defendant; and (3) it is likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision."[119] In the context of data breach litigation, this analysis largely focuses on the first two elements, injury and causation–while successfully alleging these factors sufficiently for Article III standing is relatively straightforward, many claims require greater allegations of damages and causation, and these can be stumbling blocks for data breach plaintiffs.

i. Injury & Damages

The evolution of data-breach litigation has resulted in precedent making it relatively straightforward to establish an injury in fact in the context of a data breach. Many circuits were initially skeptical of finding standing based solely on the fact of a data breach, holding that the mere possibility of future harm is not enough to support finding an injury in fact.[120] However, some circuits found that a substantial risk of identity theft will generally qualify as an injury in fact, and over time more circuits have accepted this

[117] *Id.*

[118] *E.g.*, Attias v. CareFirst, Inc., No. 15-cv-882, 2023 WL 5952052 (D.D.C. Sept. 13, 2023); In re Ambry Genetics Data Breach Litigation, 567 F. Supp.3d 1130 (C.D. Cal. 2021); Flores v. Aon Corporation, 2023 IL App (1st) 230140.

[119] Resnick v. AvMed, Inc., 693 F.3d 1317, 1323 (11th Cir. 2012).

[120] *E.g.*, Katz v. Pershing, LLC, 672 F.3d 64, 80 (1st Cir. 2012); Whalen v. Michaels Stores, Inc., 689 F. App'x 89 (2d Cir. 2017); Reilly v. Ceridian Corp., 664 F.3d 38, 40, 44 (3d Cir. 2011); Beck v. McDonald, 848 F.3d 262, 267 (4th Cir. 2017); Alleruzzo v. SuperValu, Inc., 870 F.3d 763, 766 (8th Cir. 2017).

view.[121] The risk of future injury may only establish standing sufficient to pursue injunctive relief, however, and courts have held that where parties seek monetary damages based on a data breach, they must demonstrate "a separate concrete harm caused 'by their exposure to the risk itself.'"[122]

Beyond the "injury in fact" requirement for Article III standing, many claims require further pleading to establish damages. The Ninth Circuit, for example, ruled in 2010 in *Krottner v. Starbucks Corporation* that where plaintiffs had sufficiently pled an injury in fact for Article III standing, they still fell short of pleading damages to satisfy Washington state-law claims arising from the theft of a company laptop containing the personal information of thousands of employees.[123] While the danger of future harm stemming from the release of personal data might be sufficient for Article III standing, it was insufficient for a negligence claim, which required an allegation of "actual loss" under Washington law.[124] Similarly, the D.C. District Court found in *Attias v. Carefirst, Inc.* that D.C. law required actual damages as an element of claims for breach of contract, negligence, fraud, and breach of fiduciary duty.[125] In that case, a class of plaintiffs whose data had been exposed, but not actually misused, as a result of a data breach of a health insurance provider alleged damages based on the risk of future misuse of data, a loss of the benefit of the bargain that they struck with the insurer, the cost of prophylactic measures such as identity theft protection services, and emotional distress.[126]

But in other later cases, the same types of prophylactic costs and potential future injuries have been found to be sufficient even for claims requiring actual damages. In *Sweet v.*

---

[121] *E.g.*, Remijas v. Neiman Marcus Group, 794 F.3d 688 (7th Cir. 2015); Attias v. CareFirst Inc., 865 F.3d 620, 623 (D.C. Cir. 2017); Galaria v. Nationwide Mut. Ins. Co., 663 Fed. App'x 384, 386 (6th Cir. 2016); In re Zappos.com, Inc., 888 F.3d 1020, 1023 (9th Cir. 2018). *See also* McMorris v. Carlos Lopez & Associates, LLC, 995 F.3d 295, 300-01 (2021) (holding that "plaintiffs may establish standing based on an increased risk of identity theft or fraud following the unauthorized disclosure of their data[,]" without mentioning prior unpublished decision to the contrary in *Whalen.*); *Clemens*, 48 F.4th at 153-56 (holding that "in the data breach context … a plaintiff suing for damages can satisfy concreteness as long as he alleges that the exposure to that substantial risk caused additional, currently felt concrete harms" despite prior holding in *Reilly.*).

[122] Webb v. Injured Workers Pharmacy, LLC, 72 F.4th 365, 372 (1st Cir. 2023) (*quoting TransUnion LLC v. Ramirez,* 141 S. Ct. 2190, 2211 (2021)).

[123] Krottner v. Starbucks Corp., 406 F. App'x 129 (9th Cir. 2010).

[124] *Id.* at 131.

[125] 365 F. Supp. 1, 9–11 (D.D.C. 2019).

[126] *Id.* at 11–17.

BJC Health System et al., plaintiffs sought to bring a claim against a large healthcare network that had suffered a data breach, alleging no actual misuse of their data but asserting prophylactic costs associated with credit protection services, insurance, and potential future damages associated with the exposure of their data.[127] The court relied heavily on *Dieffenbach v. Barnes & Noble, Inc.*, a Seventh Circuit decision that minimized the difference between injury in fact and actual damages in the context of a data breach, noting that where plaintiffs "have suffered an injury then damages are available[.]"[128] The *Dieffenbach* court further held that the California law applicable in that case, even an "identifiable trifle of economic injury" suffices to show damages, including credit monitoring services.[129] Based on this holding, the court in *Sweet* too held that even the minimal costs associated with ongoing identity theft protection services were sufficient to establish damages as an element of state-law claims.[130] Other circuits have similarly found minimal but measurable costs sufficient to adequately allege damages arising from a data breach.[131]

ii. Causation

For the second element, causation, only a relatively tenuous connection is required for the alleged harm to be "fairly traceable" to defendants' conduct. In the context of a data breach, "even a showing that a plaintiff's injury is indirectly caused by a defendant's actions satisfies the fairly traceable requirement."[132] In *Resnick v. AvMed, Inc.*, for example, plaintiffs merely alleged that their employers had failed to secure their information on company laptops, that those laptops were stolen, and that plaintiffs subsequently became victims of identity theft – these allegations were found to be sufficient to satisfy the "fairly traceable" requirement.[133]

As with the injury prong of standing, while minimal allegations of causation may be sufficient for Article III, successfully pleading actual claims may require more robust allegations of proximate cause. In *Resnick*, after first noting that plaintiffs had passed the

[127] 20-cv-947, 2021 WL 2661569, *2 (S.D. Ill. June 29, 2021).

[128] 887 F.3d 826, 828 (7th Cir. 2018).

[129] *Id.* at 829.

[130] *Sweet*, 2021 WL 2661569 at *5–6.

[131] Bohnak v. Marsh & McLennan Companies, Inc., 79 F.4th 276, 289–90 (2d Cir. 2023); *Clemens*, 48 F.4th at 157–78; In re U.S. Office of Personnel Management Data Security Breach Litigation, 928 F.3d 42, 64–65 (D.C. Cir. 2019).

[132] Resnick v. AvMed, Inc., 693 F.3d 1317, 1324 (11th Cir. 2012).

[133] *Id.*

low bar required for Article III causation, the court then proceed to examine whether plaintiffs had asserted proximate cause sufficiently to support their individual claims.[134] The court recognized that proximate cause required more than a simple temporal sequence of events asserting that data was exposed and that identity theft subsequently occurred – rather, plaintiffs must allege a "nexus between the two events" such as by alleging that the data used to steal a plaintiffs' identity was the same as that exposed in the breach.[135] Other circuits have similarly required a stronger causal link between a data breach and subsequent damages. The D.C. Circuit, for example, similarly found proximate cause to be satisfied where plaintiffs alleged that they had "suffered forms of identity theft accomplishable only with the type of information that [the defendant] stored and hackers accessed[,]" which "directly link[ed] the hack to the theft of the victims' private information, the pecuniary harms suffered, and the ongoing increased susceptibility to identity theft or financial injury.[136]

2. Statutory Claims

Beyond common law claims based on data breaches, individual plaintiffs may seek to assert statutory claims under a range of state and federal provisions.

In the early days of data breach litigation, there were no statutes offering claims specific to data breach. However, plaintiffs still sought to utilize state consumer protection statutes that create claims based on unfair, deceptive, or otherwise unlawful business conduct. [137] At first glance, these statutes might seem like a clumsy choice for a data breach plaintiff suing the business that has suffered a breach, as the defendant may appear more like a fellow victim than a party guilty of consumer fraud. However, over time, a common pattern for successful claims has emerged. The plaintiffs, more commonly customers of the breach target than employees, allege that they relied on representations from the entity that their sensitive customer information would be secure, while in fact

[134] *Id.* at 1325–26.
[135] *Id.* at 1327–28.
[136] *In re* U.S. Office of Personnel Management Data Security Breach Litigation, 928 F.3d 42, 67 (D.C. Cir. 2019).
[137] *Id.*

the entity was on notice as to its lax security and perhaps even failed to disclose the data breach in a timely manner, resulting in damages to the consumers.[138]

As data breaches have become a common issue, state governments have responded, and as of 2023 all fifty states, as well as the District of Columbia, Puerto Rico, the Virgin Islands, and Guam have laws that require businesses to notify affected individuals of security breaches involving personally identifiable information.[139] In theory, many of these laws do create a private right of action against businesses that fail to timely disclose a data breach.[140] In practice, however, many of these statutes leave it up to courts to determine whether a business delayed unreasonably in notifying affected parties, and even delays of weeks may not be sufficient to support a claim for failure to notify.[141]

The federal government has been slower to create laws addressing data breaches, but there are now a number of statutes and administrative provisions creating obligations for companies that suffer data breaches. Certain sectors, such as healthcare and telecommunications, have federal notification obligations similar to those imposed by state

[138] *See, e.g.*, Irwin v. Jimmy John's Franchise, LLC, 175 F. Supp. 3d 1064, 1072–73 (C.D. Ill. 2016) (finding that plaintiff had plausibly alleged a claim under the Arizona Consumer Fraud Act where she alleged that "Jimmy John's induced her and other Arizona consumers to rely on Jimmy John's deception that their financial information was secure and protected when using debit and credit cards."); In re Equifax, Inc., Customer Data Security Breach Litigation, 362 F. Supp. 3d 1295, 1336–38 (N.D. Ga. 2019) (holding plaintiffs could bring claims under numerous different state consumer fraud statutes where they alleged that "Equifax was aware of the importance of data security and of the previous well-publicized data breaches [and] despite this knowledge of cybersecurity risks, Equifax sought to capitalize on the increased number of breaches by providing identity theft protection, instead of taking steps to improve deficiencies in its cybersecurity.").

[139] *Security Breach Notification Laws*, NATIONAL CONFERENCE OF STATE LEGISLATURES (Jan. 17, 2022), https://www.ncsl.org/technology-and-communication/security-breach-notification-laws [https://perma.cc/MVA2-ACXV].

[140] *See, e.g.*, Equifax, 362 F. Supp. 3d at 1338–43 (finding plaintiffs had stated a claim under numerous state notification laws); In re Arthur J. Gallagher Data Breach Litigation, No. 22-cv-137, 2022 WL 4535092 (N.D. Ill. 2022) (finding plaintiffs had stated a claim under Illinois and California data breach notification laws).

[141] *See, e.g.*, In re Waste Management Data Breach Litigation, 2022 WL 561734 (finding that under California notifications statute, 24-day delay in notifying affected parties was not unreasonable and did not support a claim); Savidge v. Pharm-Save, Inc., No. 3:17-CV-00186-TBR, 2017 WL 5986972 (W.D. Ky. 2017) (finding that under Kentucky notification statute, a delay of nearly three weeks was insufficient to support a claim).

statutes.[142] Of these rules, the HIPAA data breach notification rule does not have a private right of action (though a HIPAA violation could support a private action brought under state law), while a private action arguably could be brought for a violation of the FCC's data breach rule.[143] The SEC has recently imposed its own cybersecurity rule requiring disclosures of cybersecurity incidents – in theory, failure to disclose an incident could now be a basis for a private action under securities laws. [144] And the Fair Credit Reporting Act (FCRA) imposes data security and breach notification requirements on its own set of covered entities.[145] The FTC, meanwhile has promulgated its own data breach notification rules that apply to certain financial institutions, in addition to its broader authority under the FTC act to pursue deceptive conduct in commerce.[146] More recently, the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) was passed into law and when fully implemented will impose data breach notification requirements on covered entities that fall into certain critical infrastructure sectors.[147] As many of these rules and statutes are new and still being implemented, there has not been sufficient time to develop case law indicating which sections might permit private actions whether any of these new rules will create significant new avenues for claims against breached companies.

---

[142] *E.g.*, 45 C.F.R. §§ 164.400-414 (the HIPAA data breach notification rule, applicable to businesses suffering a breach of unsecured protected health information); 47 CFR § 64.2011(e) (FCC data breach notification rule, governing breaches of customer proprietary network information by telecommunications carriers).

[143] *See* 47 U.S.C. § 207 (creating private right of action for injuries where a common carrier might be subject to liability under Chapter 5 of Title 47 of the U.S. Code); Global Crossing Telecommunications, Inc. v. Metrophones Telecommunications, Inc., 550 U.S. 45, 52–53 (2007) (holding that the intent of § 207 was to allow persons injuries by violations of common carriers to bring federal-court damages claims); FCC, *Fact Sheet: Data Breach Reporting Requirements at 3-5*, WC DOCKET NO. 22–21 (Nov. 22, 2023) (noting that the FCC's data breach notification rule was an implementation of 47 U.S.C. § 222, within Chapter 5).

[144] *SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies*, Press Release 2023-139, U.S. SECURITIES AND EXCHANGE COMMISSION, (July 26, 2023) https://www.sec.gov/corpfin/secg-cybersecurity#:~:text=On%20July%2026%2C%202023%2C%20the,Exchange%20Act%20of%201934%20(the [https://perma.cc/XTF2-DKAL].

[145] *See, e.g.*, 15 U.S.C. § 1681g(e).

[146] *FTC Amends Safeguards Rule to Require Non-Banking Financial Institutions to Report Data Security Breaches*, FEDERAL TRADE COMMISSION (Oct. 27, 2023) https://www.ftc.gov/news-events/news/press-releases/2023/10/ftc-amends-safeguards-rule-require-non-banking-financial-institutions-report-data-security-breaches [https://perma.cc/KV4J-472U].

[147] Consolidated Appropriations Act, 2022, PUB. L. NO. 117–103, DIVISION Y (2022).

3. Government Enforcement

In addition to private suits filed by injured parties, companies that have suffered data breaches may find themselves the target of government regulators if their conduct violated by statutes or rules regarding the treatment of data or the proper response to a data breach. On the federal side, the FTC has been most active in enforcement actions based on data breaches and in the last couple of years has undertaken numerous actions against businesses that have misled customers by failing to secure sensitive information, often charging these entities under Section 5 of the FTC Act, which bars unfair and deceptive acts and practices, as well as using its authority to enforce HIPAA and FCRA's data breach provisions.[148] State attorneys general have also begun to take note of data breaches, and as issues of data privacy and security rise in the public consciousness, more states have begun pursuing enforcement actions against companies based on violations of state level data breach notification laws.[149]

III. REMOTE WORK SCENARIOS AND EMPLOYER LIABILITY FOR DATA BREACHES

Having reviewed the current state of remote work and data breaches and the general state of the law applying to claims based on data breaches, it follows to examine how a remote workforce might influence the types of data in a breach exposed and the types of claims that employers might face. This section will accomplish this by examining a theoretical data breach through a series of linked hypothetical fact patterns that illustrate how a

[148] *E.g.*, In the Matter of Drizly, LLC, FTC Matter 2023185, Consent Order (Jan. 10, 2023) (resolving claim against Drizly under § 5(a) of the FTC Act for deceptive statements regarding data protection that caused injury after a data breach exposed customer information); United States v. Easy Healthcare Corporation, No. 23-cv-3107 (N.D. Ill. June 22, 2023) (Stipulated Order for Permanent Injunction, Civil Penalty Judgment, and Other Relief) (resolving claim against healthcare company for violation of health breach notification rule); United States v. Kohl's Department Stores, Inc., No. 20-cv-859 (E.D. Wis. June 10, 2020) (Stipulated Order for Permanent Injunction, Civil Penalty Judgment, and Other Relief) (resolving action against retailer for FCRA violation).

[149] *E.g.*, Press Release, PA. ATTORNEY GENERAL, *Attorney General Josh Shapiro Announces $8 Million Agreement With Wawa Following Investigation Into 2019 Data Breach* (July 26, 2022), https://www.attorneygeneral.gov/taking-action/attorney-general-josh-shapiro-announces-8-million-agreement-with-wawa-following-investigation-into-2019-data-breach/?mkt_tok=MTM4LUVaTS0wNDIAAAGF35R3O76Gi0gQQRIDYVgtNHglqlVilARXJESLiuI-cUEl0h0-W8XlVWalmy3U85iCeQJ9x14AIne6eEOI6gC2NhGcrbjU_ayGj7LGBrbDLSTU [https://perma.cc/Q7D8-MNYX]; Press Release, OFFICE OF THE MASS. ATTORNEY GENERAL, *Rhode Island Company To Pay $230,000 in Penalties Over Data Breach Impacting More Than 3,000 Massachusetts Residents.*

company's approach to remote work has serious implications for its potential liability in the event of a data breach.

A. The Basic Hypothetical: VPN-Based HypoCorp

1. Scenario

HypoCorp is a publicly traded, private company that manufactures a patented consumer device called an Aleph, which contain highly sophisticated proprietary code. HypoCorp has traditionally been based in Burlington, VT, yet as the company has expanded through its thriving Aleph sales, it has expanded to encompass multiple locations, including a manufacturing facility in the Philippines, a business office in New York City, a logistics hub and EU headquarters in Rotterdam, and its historic headquarters and assembly facility in Burlington.

Due to HypoCorp's increasingly spread-out workforce, it had already begun permitting remote work on a case-by-case basis prior to the Covid-19 pandemic. However, like many companies, this evolution proceeded much more rapidly with the onset of the pandemic. Now, HypoCorp permits fully remote and hybrid work arrangements for non-production employees and has relatively few employees who actually work in the office every day of the week. HypoCorp handles access for remote employees through a VPN, which is hosted on a server at the main office in Burlington. HypoCorp provides most of its professional employees with company-issued laptops. It also has a BYOD policy and requires employees to use their personal mobile devices for work. HypoCorp also permits employees to utilize personal computers for work, provided they download appropriate security software and connect to the company VPN to access company files and applications. That security software includes programs to automatically push software patches to devices used by remote workers. However, HypoCorp does not utilize monitoring software and does not have in place any programs that enable monitoring of VPN traffic.

HypoCorp regulates remote work through a number of linked policy documents that employees are required to review and sign to as a condition of employment. The first of these is the company's Appropriate Use Policy. That document states that HypoCorp provides devices and access to company applications and files (so-called "Company Technology") to employees for "legitimate business purposes" and that employees are expected to "exercise good judgment and professionalism" in their use of Company Technology. The Appropriate Use Policy states that Company Technology should not be

used for personal purposes and that HypoCorp maintains ownership over Company Technology and all data sent, received, and stored with Company Technology. The Company reserves the right to inspect, monitor, and record employees' use of company technology, and by agreeing to the Acceptable Use Policy employees waive any expectation of privacy with respect to their use of Company Technology.

Second, HypoCorp utilizes a BYOD Policy to govern employee use of personal devices for work. That policy states that HypoCorp permits and encourages employees to use personal electronic devices for work, but it notes that such devices must be used in a sensible, productive, ethical, and lawful manner to protect both HypoCorp and employees. The BYOD Policy, as with the Appropriate Use Policy, reserves HypoCorp's right to monitor all HypoCorp content or all contents of a BYOD device, requiring employees to disclaim any expectation of privacy in such a device as a condition of its use as a BYOD device for any HypoCorp purposes.

In March 2023, a sophisticated gang of hackers based in Moldova targeted HypoCorp with a wave of targeted spearfishing attacks. Most attempts to gain access to HypoCorp systems were unsuccessful, but the hackers were able to gain access to an email account belonging to a low-level Burlington-based sales rep. Using access to the sales rep's email, the hackers were able to target the email account of a high-ranking systems administrator, gaining access to the administrator's computer. From that computer, using the administrator's access to HypoCorp systems, the hackers were able to begin planting their code and applications throughout HypoCorp systems, creating numerous back doors into HypoCorp servers. Over the next month, the hackers gradually obtained greater access to and control over HypoCorp systems, gaining access to most company files as well as to HypoCorp's VPN server. As employees connected communicated by email, connected to HypoCorp's servers and used the HypoCorp VPN, the hackers planted code on a wide array of employer-issued devices and employee personal devices.

This wide-scale breach and extensive monitoring was part of an effort to gain access to the proprietary code used on HypoCorp's Aleph devices. That code, which was closely guarded and kept on a separate server, was not breached, though draft sections of code that were under development were revealed through emails between company staff that hackers obtained. While the hackers did not ultimately obtain the full Aleph code, they did gain access to a wide range of sensitive company documents, including employee social security number and bank account information and sensitive information about company clients. Through their access company networks, the hackers also obtained access to the

personal financial accounts, emails, and social media accounts of a number of employees who conducted personal activities while connected to the HypoCorp VPN. The hackers sought to use their access to the HypoCorp VPN to monitor traffic, though the lack of existing VPN monitoring tools slowed this process, and it took several months before the hackers were able to put code in place permitting monitoring of VPN traffic. Similarly, the limited remote patching tools previously in place on HypoCorp's employer-issued devices did not facilitate the spread of malware, slowing the spread of the breach to new devices.

Ultimately, after several months of burrowing into HypoCorp systems failed to result in access to the sought-after Aleph code, the hackers decided to monetize the access that they already had before a potential discovery of their activity might spoil their plans. On August 19, 2023, the hackers locked all infected systems on the HypoCorp network with a ransomware script, threatening to delete all data and expose sensitive information relating to HypoCorp, its employees, and its customers if the ransom was not paid. HypoCorp promptly retained the services of data breach specialists, who were able to regain access to certain elements of HypoCorp's systems. Ultimately, the ransomware was circumvented, and HypoCorp was able to regain full control over its systems by the end of October 2023. While some employees were able to resume work in the intervening period relying on backups on local servers, the shutdown of HypoCorp's VPN severely complicated operations for HypoCorp's remote workforce for several weeks until a viable alternative could be put in place. The hackers also leaked embarrassing information about HypoCorp and its customers and posted sensitive employee information for sale on the dark web.

Shortly after the data breach was publicly disclosed, a class of employees sued HypoCorp for damages resulting from the breach. HypoCorp is also facing lawsuits from unhappy former customers and inquiries from state and federal regulators.

2. Analysis

This scenario shows the dangers of a data breach to any institution, even one that manages remote work responsibly. Here, much of the damage resulting from the breach could have occurred regardless of whether employees were working remotely or were entirely in-person in a single office–a spear-fishing attack is a common start to a data

breach, and does not depend on a remote workforce.[150] Once an attack has accessed a system, a significant amount of sensitive data can easily be exposed regardless of whether that system has enabled remote access.[151] Here, having a hybrid workforce did ultimately exacerbate the consequences of the breach–as studies have shown,[152] the remote workers at HypoCorp conducted more personal activities on company-issued devices and mixed personal and work activities on BYOD devices, resulting in somewhat greater exposure of personal information than what might have been contained solely in HypoCorp's personnel files. The company's use of a VPN to enable remote access also ultimately permitted the hackers to monitor some traffic through the VPN, though the same could had occurred with a single-office workforce had hackers gained access to an office server–perhaps more importantly, when the hackers initiated their ransomware attack, the fact that HypoCorp's workforce was remote and relied heavily on remote access meant that the attack created greater disruption than might have been the case for an in-person workforce.

What would be the legal ramifications for a breach like the one seen in this scenario? Based on applicable Second Circuit law, employees would have little difficulty establishing standing to sue, even if the exposed data had not yet been misused.[153] The simplest claims for the aggrieved employees to bring would be common law tort claims such as negligence. For a basic negligence claim, the employees would need to demonstrate that HypoCorp had failed to exercise due care in collecting and storing data. Similarly, employees could seek to assert implied breach of contract, arguing that by agreeing to hand over their data and consenting to HypoCorp's Acceptable Use and BYOD policies, they had received an implicit assurance that HypoCorp would protect their information and not abuse its access to their devices.[154] Thus these policies, supposedly intended to protect the company, might well work against them in data breach litigation. Again, the employees would need to show that HypoCorp had failed to use reasonable measures to protect employee data.

[150] *What is Spear Phishing?*, IBM, https://www.ibm.com/topics/spear-phishing [https://perma.cc/G45T-QF67] (last visited April 12,2024).

[151] *Id.*

[152] *See* Jose Maria Barrero et al., *supra* note 28.

[153] *E.g.*, Bohnak v. Marsh & McLennan Companies, Inc., 79 F.4th 276, 289–90 (2d Cir. 2023).

[154] *See generally* Bohnak, 79 F.4th 276.

Both claims would turn on a court's perception of whether HypoCorp acted in a reasonable manner in its efforts to protect its systems and secure data[155] – here, there is no indication that HypoCorp's security was necessarily lacking. Even the best security systems are vulnerable to human error, and spearfishing attacks are specifically designed to exploit these errors.[156] Plaintiffs could seek to fault HypoCorp's use of a VPN to enable remote access, pointing to how the hackers were ultimately able to utilize the VPN to gain further information, but success in relying on the VPN would likely depend on the VPN's security – part of the reason why VPNs are popular is that they allow companies to encrypt traffic. As HypoCorp had an effectively secured VPN and had not enabled easy monitoring of VPN traffic, the fact that hackers that gained access via spearfishing were ultimately able to access the VPN might not be the kind of failure that would support a claim of negligence or implied breach of contract. Perhaps more concerning than the fact of access itself is the fact that HypoCorp never detected the breach and only became aware of the problem when the hackers initiated their ransomware attack, roughly five months after the initial access. While HypoCorp could certainly argue that even with strong security, it was unable to detect the breach, this delay certainly would present plaintiffs with an opportunity to argue that HypoCorp's security was lacking and that it should have detected the breach sooner.

The same factual debate surrounding the adequacy of HypoCorp's security (and whether it was on notice as to any security failings) would inform the success or failure of any state consumer fraud action, which might also examine the timeliness of HypoCorp's response to the attack and its disclosure to affected parties and public.[157] A perceived tardy disclosure of the attack could also permit a private claim under a state data breach notification law, yet as discussed *supra*, these statutes often give courts discretion to determine when a delay in reporting is reasonable, and many courts have permitted reporting of data breaches weeks after the facts of a breach became known.[158]

This scenario represents a version of a data breach in which HypoCorp has acted relatively responsibly in attempting to create a secure environment for remote work, and as a result relatively little has played out differently as a result of remote work. Here, most of the legal consequences of the attack would be largely the same if HypoCorp had

[155] *See id.*
[156] *See id.*
[157] *See id.*
[158] *See infra* Section IV(A).

all of its employees working in person in a single office. The practical ramifications of the incident do appear to have been greater here as a result of HypoCorp's remote workforce, which found itself much more cut off from coworkers and resources a local workforce would have, and perhaps slightly more sensitive employee data was revealed due to HypoCorp's greater use of BYOD devices for remote workers. Overall, HypoCorp will likely suffer consequences not significantly worse than would be expected for any similarly placed enterprise, regardless of remote work status – as the following scenarios show, changes to the fact pattern can cause this outcome to shift drastically, leading to much greater complications resulting from a remote workforce.

B. Variation 1: Cloud-based HypoCorp

1. Scenario

In this scenario, the basic facts about HypoCorp, its employees, and its internal policies are unchanged. However, rather than using a private VPN on a company server to allow access to data and applications hosted by HypoCorp, in this scenario HypoCorp enables remote work by using a cloud-based system, contracting with a major multinational tech company called Cloudly for server space. All HypoCorp employees access remote desktops and applications that are hosted by Cloudly, either from personal or company-issued devices. To the extent that IT support or technical updates are needed for either company-issued or personal devices, that support is handled by Cloudly, which has limited access to those devices.

In this scenario, in June 2023 HypoCorp is notified by the cloud provider of a breach affecting HypoCorp data and applications. The cloud provider says that it is working to identify the scope of the breach, but is not wholly forthcoming about its investigation, leaving HypoCorp uncertain as to precisely what information has been breached. HypoCorp retains experts who review its own internal systems and confirms that the breach of the cloud provider did not spread to HypoCorp's own systems. As HypoCorp uses the cloud provider for the vast majority of its computing needs, it is not able to immediately transition to a new system, though in less than three weeks, using backup data, it has transitioned to an alternate system that no longer relies on the cloud provider. This transition, however, is extremely disruptive, resulting in significant overtime for employees and disgruntled clients.

HypoCorp continues to press Cloudly for details of what information might have been exposed. The appearance of certain HypoCorp files with sensitive customer and employee

data for sale on the dark web provides some indication of what information may have been taken, but HypoCorp is uncertain that this disclosure is related to the breach at Cloudly.

It is not until October of 2023 that Cloudly gives HypoCorp the full details of the breach, stating that access occurred over an extended period between December 2022 and February of 2023 and resulted in access to substantially all HypoCorp files stored by the cloud provider as well as permitting monitoring of HypoCorp employees' usage of cloud-based apps. Once again, the hackers did not gain access to HypoCorp's closely guarded Aleph code, which was not stored with Cloudly. However, they did gain access to company personnel files and customer data, which were released online. While the hackers were able to monitor HypoCorp employees' use of cloud-based applications, this revealed little personal information, as relatively few employees used cloud applications for personal purposes.

Once again, a class of employees sued HypoCorp for damages resulting from the breach. HypoCorp also faces lawsuits from unhappy former customers and inquiries from state and federal regulators.

2. Analysis

This scenario demonstrates the extent to which a business may effectively outsource its security and the responsibility for creating a reliable method of remote access by using a cloud provider, and it shows how this outsourcing may have both positive and negative effects. Many businesses, particularly smaller enterprises, choose to rely on cloud providers for remote access due to the complexity of creating and also maintaining a secure VPN that ensures reliable access to applications and data for remote workers.[159] Cloud providers, most of which are large, well-known corporations, are perceived as having the specialized personnel necessary to create the most secure access.

However, the mere fact that cloud providers are large, well-established companies with many employees dedicated to cybersecurity does not make them immune to data breaches – even the largest cloud providers such as Amazon have suffered their own data breaches

[159] *See* IBM, *supra* note 150.

that have exposed cloud customer data.[160] In 2022, for example, a former Amazon Web Services employee was convicted of having misused her access to steal data and computer power from clients of Amazon's cloud services, resulting in a breach that affected more than 100 million customers of the bank Capital One and resulted in Capital One paying over $270 million in fines and settlements.[161] While these breaches may occur infrequently, when they do happen they may leave affected businesses in an even worse position than if they had managed remote access themselves, dependent on the cloud provider for information and lacking a clear picture of what information was exposed and whether the attack has been contained.

This is the situation that HypoCorp faces here when the breach occurs – it finds itself with limited facts, uncertain as to the extent of the breach and how to respond. It does not obtain a full picture of the damage until months after the event, leaving it uncertain as to what it should tell employees and customers. On the other hand, the use of a cloud provider does compartmentalize the breach, limiting the types of data exposed to that which HypoCorp chose to store on the cloud. The amount of employee activity that is open to monitoring is also reduced, as only those applications accessed through the cloud are exposed – in general, employees conduct fewer personal activities on these applications, and there is less incidental exposure of personal employee information than in the VPN-based scenario.

How does this cloud-based scenario change HypoCorp's legal vulnerability? On the one hand, the potential damages from private claims like negligence, implied breach of contract, and consumer fraud are likely to be more limited, as the amount of data exposed is less significant. On the other hand, HypoCorp is perhaps in a worse position in arguing that its security was adequate and that it used reasonable measures to protect data. Here, HypoCorp has simply placed responsibility for cloud security with Cloudly, and it appears to have had little oversight into how its data was protected, trusting in the size and reputation of its cloud provider. A court might well find this to be insufficient, particularly if Cloudly had suffered any prior data breaches that should have given HypoCorp pause had it done its homework. What's more, the slow reveal of the facts of the Cloudly's data breach leaves HypoCorp vulnerable to claims based on breach

[160] Press Release, DEPARTMENT OF JUSTICE, *Former Seattle Tech Worker Convicted of Wire Fraud and Computer Intrusions* (June 17, 2022), https://www.justice.gov/usao-wdwa/pr/former-seattle-tech-worker-convicted-wire-fraud-and-computer-intrusions [https://perma.cc/X35H-DZ6J].

[161] *Id.*

notification laws, as it may have delayed an unreasonable amount of time to notify customers and employees as it waited for details of the attack from Cloudly. In sum, this scenario illustrates how cloud-based remote access can in theory mitigate risk and reduce an organization's costs and tech burden in creating remote access, but excessive reliance on a cloud provider can lead to complacency, ultimately making an organization more vulnerable to breaches and liability.

C. Variation 2: Monitoring at HypoCorp

1. Scenario

For this scenario, the basic facts surrounding HypoCorp are unchanged, and as in the initial scenario HypoCorp has chosen to utilize a VPN-based system to enable remote access by employees. The main difference is that in this version of events, HypoCorp has chosen to enable and engage in extensive monitoring of employee activity. HypoCorp's workforce was once a tightly knit group of coworkers, united by the company's startup atmosphere and consolidated in a single, small office in Burlington, VT. As the company has grown, as its headcount has increased, and as employees have spread out among different offices and remote locations around the globe, that tightly knit atmosphere has dissipated, and rather than feeling like an energetic start-up, HypoCorp has come to feel like an established corporation with a certain loss of employee enthusiasm and buy-in. This perceived loss of connection and employee sentiment concerns executives, particularly in the wake of the Covid-19 pandemic, as large numbers of employees continue to work remotely from home, without any regular face-to-face contact with coworkers and management.

Ultimately, HypoCorp executives decide to utilize workplace productivity programs that enable monitoring of employee computer activities and to actively engage in employee monitoring on both company-issued and BYOD devices. HypoCorp executives do this based on the consent already given by their employees upon accepting the company's Acceptable Use and BYOD policies upon employment; they do not notify employees of the new monitoring; monitoring software is installed on devices under the guise of software updates without explanation of its purpose. HypoCorp also installs VPN monitoring applications on the VPN server, enabling more active monitoring of all traffic on the VPN.

Employees gradually become aware of surveillance as managers raise productivity concerns during performance review meetings and appear aware of employees' use of

devices for personal purposes, citing specific websites that have been accessed. Unfortunately, this surveillance does not have the desired effect of increasing productivity – while some particularly inefficient employees are sufficiently frightened after being called out on their use of online streaming services during work hours, many employees find the rumors of surveillance to be off-putting and come to distrust management. As in other businesses that have engaged in surveillance, HypoCorp finds that employee knowledge of monitoring does not lead them to cease personal activities on device used for employment. To the contrary, some employees seem to increase their use of work devices for personal purposes, perhaps in a show of defiance at the unpopular policy.

These surveillance programs have significant ramifications when the breach occurs – while in the initial scenario it took the hackers a significant amount of time and effort to use access to the VPN server to engage in surveillance of VPN traffic, in this scenario the hackers are able to use existing tools to monitor activity across virtually all devices, company-issued and personal, that have been used for work at HypoCorp. This allows the hackers to amass much more sensitive data – they are able to monitor the select group of programmers who patch and maintain the code for HypoCorp's Aleph device, giving the hackers much greater insight into this crown jewel of the company. More broadly, the existence of employee monitoring tools makes it much easier to view all of the activity of any particular employee of HypoCorp, and HypoCorp's dissatisfied workforce spends more time on a greater range of personal activities, resulting in greater incidental exposure of personal information of employees in addition to the company information that was the main target of the breach.

The aftermath of the data breach plays out much the same as in the other scenarios, with disgruntled employees and frustrated customers. The revelation that HypoCorp's own monitoring practices exacerbated the attack, however, fuels further public anger and leads to greater interest from regulators.

2. Analysis

This final fact pattern serves to illustrate what might be considered a worst-case scenario, one which illustrates all of the possible complications that a remote workforce can have in the event of a data breach. Here, in contrast to the preceding two scenarios, the legal and practical consequences of the data breach are clearly much worse than would have been the case with a non-remote workforce because of specific choices that the company has made about the way that it has handled remote work.

The most obvious difference here is the use of employee surveillance – by creating tools specifically designed to monitor employees, HypoCorp has effectively placed those tools in the hands of the hackers once the breach has occurred. Further, the simmering distrust of HypoCorp's employees and their dissatisfaction to the company has led to more employees conducting personal activities on company-issued and BYOD devices. The combination of these two factors results in much greater personal employee information being revealed than in either of the other remote-work scenarios. In all probability, these factors result in far greater exposure of employee personal data than would be the case if HypoCorp had a fully in-person workforce. However, beyond the exposure of employee personal data, this scenario demonstrates how employee surveillance and poor management of remote access protocols can lead to much greater loss of customer data and far greater damage to the business as a whole.

The legal and practical consequences of the breach in this scenario would be significant. Both employee and customer plaintiffs would likely find it much easier to argue that HypoCorp's security was deficient when it purposefully put in place powerful surveillance tools that ultimately enabled the hackers to spy on its own employees and steal personal information and business data. What's more, the way that HypoCorp has acted in this scenario makes it far less sympathetic as a victim of the breach – rather, the hostile tone of HypoCorp's relationship with its employees creates a narrative where HypoCorp looks like an overbearing, reckless corporation, emphasizing productivity and profits over the safety of its employees' and customers' data. This type of narrative is likely to appeal to state and federal regulators, and HypoCorp is far likely to face more aggressive enforcement action in this scenario. Perhaps most importantly, HypoCorp's weak internal security resulted in the exposure of its crown jewel, its proprietary Aleph code, a loss that might well prove crippling in the marketplace.

IV. PROPOSALS FOR REFORM

The hypothetical scenarios in the preceding section are intended to demonstrate first that there are many ways of managing the risk associated with data breaches in an enterprise relying on remote workers. Remote access can be created in a relatively safe and responsible fashion, or a company can misuse remote access in ways that leave it far more vulnerable in the event of a data breach. Secondly, the preceding scenarios demonstrate how the responsibility for determining what type of remote work and remote access arrangements are suitable falls largely on private companies, with relatively few guardrails currently created by state or federal law. This section will explore first what companies

should do on their own to ensure that their approach to remote work is not negligent, and secondly what legislators could do to ensure that businesses make the right choices in how to enable remote access for their employees.

A. Internal Measures

Most employers have probably already been lectured on best practices for ensuring adequate cybersecurity, but they bear repeating. Organizations must ensure that employees are comprehensively educated in the risks associated with data breach, including the risk of social engineering attacks such as spearphishing. Organizations should have updated data security standards and be conscious of the ways that data are used and stored. Organizations should have dedicated personnel to monitor cybersecurity and ensure that security systems are up to date. And organizations should back up critical data to ensure continuity in case data is deleted or access is lost as a result of a breach.

All of these are excellent principles for any organization to use to ensure adequate cybersecurity, regardless of whether it utilizes remote workers or not. But these principles must be taken a step further in a hybrid organization with a large remote workforce – employees should be educated not merely in the general risks associated with hackers and phishing, but also in how their remote work creates additional risk. This includes a clear discussion of how use of personal devices or personal activities conducted on company devices risks exposing personal data to would-be hackers targeting the company. For their part, organizations constructing remote access architecture must consider the potential ramifications in the event of a breach. If a company is considering a comprehensive BYOD policy, requiring employees to work remotely on their own personal laptops and cellphones, it should consider whether it is unintentionally making itself a custodian of a large amount of employee personal information that it might accidentally expose in a breach. Similarly, companies should consider the effects of a data breach in determining how to construct their VPNs or whether to utilize a cloud service provider – any remote access setup should be selected not merely with an eye to external security but also with consideration of how to compartmentalize a breach and limit access to sensitive company documents and employee data. With this in mind, programs designed to surveil employees seem particularly risky, purposefully creating tools that have significant potential for misuse if they fall into the wrong hands. Companies should consider the research

indicating that these programs are in fact ineffective at increasing worker productivity and abandon them.[162]

B. Legislation

While some organizations will choose to responsibly manage remote work of their own accord, some inevitably will not. It falls to legislators to take steps to mandate businesses to make the right decisions and instill proper standards in the marketplace. How can law construct proper data protection principles in the context of remote work? What is required to protect individuals from the kinds of practices, injurious to personal data privacy, described in the preceding scenarios? A comprehensive data privacy framework is needed, one that goes beyond many existing consumer protection laws in protecting not merely *consumers*, but also *employees*. But employment is a nebulous concept encompassing a web of different relationships, formal and informal[163] – to truly ensure that the full scope of these interactions benefit from any data protection framework, the framework must be truly comprehensive, covering all individuals, regardless of their status as consumers or employees. All individuals should have privacy rights in their own data, and to protect those privacy rights, obligations must be imposed not merely on those who consciously purchase, use, or store personal data of individuals, but of all those who, intentionally or not, possess access to that data. This group of those individuals and entities who possess access to protected data may be referred to as "processors" and the law must set clear standards for how processors may interact with personal data, not merely requiring that businesses act "responsibly" and creating the possibility for retroactive liability when things go wrong, but giving businesses guiding principles that allow them to calculate what systems are likely to constitute responsible practice.

The best examples of regulatory systems that create data rights for individuals and impose clear data protection standards on processors can be seen in the EU and its member states, which have instituted the most comprehensive data privacy laws in

---

[162] *See, e.g.*, Paresh Dave, *Employees Assume Bosses Track Their Work Computers, Survey Finds*, L.A. TIMES (May 23, 2013), https://www.latimes.com/business/technology/la-fi-tn-employees-computer-monitoring-20130522-story.html [https://perma.cc/B7CM-SJJ4]; Chase Thiel et al., *Monitoring Employees Makes Them More Likely to Break Rules*, HARV. BUS. REV. (June 27, 2022), https://hbr.org/2022/06/monitoring-employees-makes-them-more-likely-to-break-rules [https://perma.cc/6WER-AW3U].

[163] *See generally*, DAVID MARSDEN, 'THE EMPLOYMENT RELATIONSHIP', A THEORY OF EMPLOYMENT SYSTEMS: MICRO-FOUNDATIONS OF SOCIETAL DIVERSITY (Oxford, 1999).

existence today. The General Data Protection Regulation (GDPR), adopted in 2016, is commonly regarded as the strictest data protection law in the world and protects natural persons "with regard to the processing of personal data and rules relating to the free movement of personal data."[164] The GDPR requires that companies process personal data "lawfully, fairly and in a transparent manner[]" that data be "collected for specified, explicit and legitimate purposes" and that any data collection be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed[.]"[165] In an employment context, this means that an employer must have sound legal and practical justifications for collecting and processing employee data, and those justifications for collection and processing must be continually balanced against an employee's right to privacy. A similar balancing test can be seen under the European Convention on Human Rights, in which Article 8 establishes the right to privacy. In *Case of Barbulescu*, for example, the European Court of Human Rights in 2017 applied a Romanian data privacy law as well as Article 8 of the ECHR, finding that in weighing the permissibility of employer monitoring of employees, courts should look to: [166]

- Prior notification of employees of potential monitoring;
- The extent of monitoring and the degree of intrusion into employee privacy;
- Whether there are legitimate reasons to justify monitoring;
- Whether monitoring could be accomplished by less intrusive methods;
- The consequences of monitoring for the employee and the employer's purpose of the monitoring;
- Whether the employee was provided with adequate safeguards to protect privacy.

The GDPR has some elements that appear to go beyond this ECHR balancing test, emphasizing that consent to any data transfer must be freely given after a clear request for consent.[167] In sum, businesses in Europe already have a comprehensive regulatory scheme governing data privacy, and they have clear sets of factors to look to in assessing

[164] General Data Protection Regulation, art. 1.

[165] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 35 [hereinafter GDPR].

[166] *See* Bărbulescu v. Romania, App. No. 61496/08, ¶ 121 (Sept. 5, 2017), https://hudoc.echr.coe.int/fre?i=001-177082 [https://perma.cc/H7NM-ZHX3].

[167] *See* GDPR, *supra* note 165, at 37.

whether their remote access protocols are acceptable. European data privacy principles require that any policy of employee monitoring be finely balanced and well justified, and some employers who have aggressively pursued the kinds of employer surveillance technologies discussed in this paper have already been penalized.[168] As a result employment counsel are already encouraging EU employers to limit or avoid employee monitoring and strictly comply with the GDPR in storing employee data.[169]

The United States is well behind Europe in passing comprehensive privacy laws similar to the GDPR. Thus far, data protection laws in the United States, to the extent that they exist, are highly fragmented. On the federal level, there are no overarching data security standards, only sectoral standards like HIPAA for the health care industry and the FCC's rules for telecommunications providers.[170] Even in academia, the debate surrounding data privacy has often fixated on particular industries or bad actors, singling out major tech companies, while ignoring the access to data that the average small or midsized employer now possesses.[171] Those commentators who have called for comprehensive data privacy reforms, but unlike the GDPR and ECHR data protection regimes, these proposals do not come with a clear enumeration of factors for businesses to consider in crafting data

[168] *See, e.g.*, Mauro Orru, *Amazon Fined in France over Alleged Employee Surveillance*, WALL ST. J., https://www.wsj.com/tech/amazon-fined-in-france-over-alleged-employee-surveillance-74cd20a3 [https://perma.cc/D4R6-QRV6] (Jan. 23, 2024, 7:10 AM).

[169] *See, e.g.*, Christian Schröder & Nicholas Farnsworth, *Increased Scrutiny of Employee Monitoring Practices: Top 6 Takeaways Employers Need to Know*, ORRICK (Sept. 22, 2022), https://www.orrick.com/en/Insights/2022/09/Increased-Scrutiny-of-Employee-Monitoring-Practices-Top-5-Takeaways-Employers-Need-to-Know [https://perma.cc/LL3G-7HNT]. *See also* Kara K. Trowell, *Proceed with Caution when Remotely Monitoring Employees in the EU*, SHRM (Nov. 20, 2020), https://www.shrm.org/topics-tools/news/proceed-caution-remotely-monitoring-employees-eu [https://perma.cc/67WZ-JZV7].

[170] *See* F. PAUL PITTMAN ET AL., DATA PROTECTION LAWS AND REGULATIONS (Tim Hickman & Detlev Gabel eds., 2023), https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa [https://perma.cc/293C-DAZL].

[171] *See, e.g.*, Lina M. Khan & David E. Pozen, *A Skeptical View of Information Fiduciaries*, 133 Harv. L. Rev. 497, 498 (2019) (rejecting the broad theory of data protection in favor of focus on the "more fundamental problems associated with outsized market share" of "dominant online platforms[.]"). *See also* Kiel Brennan-Marquez, *Beware of Giant Tech Companies Bearing Jurisprudential Gifts*, 134 Harv. L. Rev. F. 434, 434 (2021) (discussing the "rapacious approach to data surveillance" adopted by "giant tech companies[.]").

protection policies, instead calling for new duties without clear guidelines on how to avoid breaching them.[172]

There are state laws that purport to establish broader standards, but these state efforts result in a geographic patchwork of different standards and often create vague obligations that do little to build on existing case law. A number of states, for example, have recently adopted "comprehensive" data privacy statutes requiring businesses that own or store personal information to use reasonable measures to protect that data.[173] But these supposedly comprehensive state statutes are highly circumscribed in a number of ways – they often apply only to extremely large businesses, using thresholds like gross annual revenue[174] or number of individuals whose data the business processes.[175] And most of these laws apply only to consumers, exempting employees statutory protections.[176] In sum, most of these laws will do little to prevent potential misuse and exposure of employee data.

The state statute that goes furthest towards creating broad data protection is California. The California Consumer Privacy Act ("CCPA"), passed in 2018, attempts to replicate

[172] *See, e.g.*, Jack M. Balkin, *The Fiduciary Model of Privacy*, 134 Harv. L. Rev. F. 11, 14 (2020). Balkin calls for digital platforms to be recognized as "information fiduciaries," with the traditional fiduciary duties of care and loyalty as well as a duty of confidentiality. But this theory is merely an evolution of existing judicial law finding that platforms have a duty of reasonable care towards those whose data they collect, and like that statute it provides businesses with few palpable guidelines or factors to help assess how to meet these weighty duties in the context of ever-evolving Internet and computer systems.

[173] These states and territories include Maryland, New York, Virginia, Delaware, and the District of Columbia. MD. CODE ANN., COM. LAW §§ 14-3503–3508 (West through 2023 Reg. Sess.); N.Y. GEN. BUS. LAW § 899-bb (Consol., Lexis Advance through 2024 released Ch. 1-49, 61-105); UTAH CODE ANN. §§ 13-61-101-–404 (Lexis through the 2d Spec. Sess. laws of 2023); COLO. REV. STAT. § 6-1-1301–1313 (Lexis Advance through Ch. 38 of the 2024 Reg. Sess., effective as of March 22, 2024); S.B. 6, 2022 Reg. Sess. (Conn. 2022); VA. CODE ANN. § 59.1-575 (Lexis Advance through 2023 Spec. Sess. I); S.F. 262, 90th Gen. Assemb. (Iowa 2023); 2023 Ind. Acts 1050; Tennessee Information Protection Act, S.B. 73, 113th Gen. Assemb. (Tenn. 2023); S.B. 384, 68th Leg. (Mont. 2023); S.B. 262, 2023 Leg., Reg. Sess. (Fla. 2023); H.B. 4, 88th Reg. Sess. (Tex. 2023); S.B. 619, 82d Leg. Assemb., Reg. Sess. (Or. 2023).

[174] *See, e.g.*, S.B. 262 § 501.702(9)(a)(5), 2023 Leg., Reg. Sess. (Fla. 2023) (setting a threshold of $1 billion in global gross annual revenue for the definition of a data "controller").

[175] *See, e.g.*, COLO. REV. STAT. § 6-1-1304(1)(b)(I) (Lexis Advance through Ch. 38 of the 2024 Reg. Sess., effective as of March 22, 2024) (defining "controller" for statutory purposes as a business that "controls or processes the personal data of one hundred thousand consumers or more during a calendar year").

[176] *See, e.g.*, UTAH CODE ANN. §§ 13-61-101-(10)(b) (Lexis through the 2d Spec. Sess. laws of 2023) (exempting "individual[s] acting in an employment or commercial context" from statutory protections for consumers).

some of the data protection provisions of the GDPR, with slightly lesser scope. It was subsequently amended and expanded by the California Privacy Rights Act ("CPRA"), which passed as a ballot proposition in 2020.[177] The CCPA, as amended by CPRA, applies only to residents of California and does not require prior consent or other legal authorization for data processing, merely requiring businesses to notify employees about the types of personal information that employers collect, as well as giving employees the right to delete personal information collected from them and opt out of any sale or sharing of their personal data, among other things.[178] The CCPA also only applies to businesses above a size threshold, rather than applying to all employers.[179] Most importantly, like many U.S. data privacy laws, the CCPA initially exempted personal data of a business's employees from the scope of the law, though that exemption expired on January 1, 2023, when CPRA's provisions took effect.[180]

Ultimately, California's privacy laws are still limited – they apply only to individuals in California and to businesses active in California, they still retain a size threshold for businesses, and they lack the requirement of a prior legal justification for data processing, as well as the balancing test seen in the GDPR and the ECHR jurisprudence.[181] However, these laws and the other recently passed comprehensive state privacy laws are steps in the right direction. If expanded on a state-by-state basis across the country, or preferably in federal legislation that would have a national effect, a comprehensive set of data privacy rules applying to employees as well as consumers would likely have the salutary effect of making employers think twice about engaging in ineffective and dangerous practices such as employee monitoring, or at least think much more carefully about the scope of any monitoring program and encourage more responsibility in creating remote access protocols. The American Law Institute has taken an important step away from fragmented, sectoral data privacy laws in the US and rather towards a broader, truly comprehensive framework. In its 2020 Principles of the Law of Data Privacy, the ALI incorporates existing U.S. data privacy laws as well as taking inspiration from the EU to craft a set of "fair information practice principles" or FIPPs.[182] These FIPPs include well fleshed-out discussions of expectations for consent, data retention and destruction, and

[177] *See* The California Privacy Rights of 2020, Proposition 24 (Cal. 2020).
[178] *See* CAL. CIV. CODE §§ 1798.100, 1798.105 (Deering, Lexis through 2024 Reg. Sess. Ch. 1).
[179] *See* CAL. CIV. CODE § 1798.140(d)(1) (Deering, Lexis through 2024 Reg. Sess. Ch. 1).
[180] *See* CAL. CIV. CODE § 1798.145(m)(1) (Deering, Lexis through 2024 Reg. Sess. Ch. 1).
[181] *See* CAL. CIV. CODE §§ 1798.100, 1798.140(d)(1) (Deering, Lexis through 2024 Reg. Sess. Ch. 1).
[182] *See* THE AM. L. INST., PRINCIPLES OF THE LAW — DATA PRIVACY 9 (2020).

data security and data breach notifications.[183] If utilized by judges and regulators, these kinds of global principles could provide much needed guidance and factors for businesses to look to beyond the vaguely worded "reasonableness" standards present in existing statutes and case law. State legislators can look to these principles as well as drawing inspiration from European law in seeking to craft broader data privacy provisions, and hopefully federal legislators can build on these efforts as well in federal legislation, which would ultimately be the best way to ensure a clear, consistent set of regulations that put businesses on notice of what is expected of them.

For now, however, businesses are largely on their own in the U.S. in making key decisions regarding how to manage and secure remote access for hybrid and remote employees, deciding for themselves what methods of constructing access are "reasonable" from a data security perspective, and employees can do little but live with the choices that their employers make.

V. CONCLUSION

The nature of remote work continues to evolve, and the battle against data breaches is an ever-evolving struggle against an amorphous enemy. Businesses must be conscious of the impact that their decisions regarding remote work may have on their access to employee data and their potential liability in the modern online economy, or they risk finding themselves adrift in a storm, like the hapless tugboats in the *T.J. Hooper*. For their part, state and federal legislators should look to Europe in seeking models for new laws that will force companies to exercise common sense in constructing secure remote access protocols and minimizing the potential exposure of employee data.

[183] *See id.* at 49–56, 76–93.