EFiled: Sep 16 2022 12:56PM EDT
Transaction ID 68113963
Case No. 2022-0819-

IN THE COURT OF CHANCERY OF THE STATE OF DELAWARE

JENNA HARPER,

Derivatively on behalf of T-Mobile US, Inc.,

Plaintiff,

v.

G. MICHAEL SIEVERT, TIMOTHEUS HÖTTGES, MARCELO CLAURE, SRIKANT M. DATAR, CHRISTIAN P. ILLEK, RAPHAEL KÜBLER, LETITIA A. LONG, THORSTEN LANGHEIM, DOMINIQUE LEROY, TERESA A. TAYLOR, OMAR TAZI, KELVIN R. WESTBROOK, BAVAN HOLLOWAY, MICHAEL WILKENS, SRINI GOLAPAN, LAWRENCE H. GUFFEY, and RONALD D. FISHER,

Defendants,

and

T-MOBILE US, INC.

Nominal Defendant

C.A. No. ______ - _______

**VERIFIED SHAREHOLDER DERIVATIVE COMPLAINT**

Plaintiff Jenna Harper, derivatively on behalf of nominal defendant T-Mobile US, Inc. (“T-Mobile” or the “Company”), brings the following Verified Stockholder Derivative Complaint against T-Mobile directors G. Michael Sievert, Timotheus

Höttges, Marcelo Claure, Srikant M. Datar, Christian P. Illek, Raphael Kübler, Letitia A. Long, Thorsten Langheim, Dominique Leroy, Teresa A. Taylor, Omar Tazi, Kelvin R. Westbrook, and Bavan Holloway (collectively, the "Director Defendants") and former T-Mobile directors Michael Wilkens, Srini Golapan, Lawrence H. Guffey, and Ronald D. Fisher (collectively, the "Former Director Defendants" and, together with the Director Defendants, the "Individual Defendants"). The allegations of this Complaint are based on the knowledge of Plaintiff as to herself, and on information and belief, including the investigation of counsel and review of publicly available information including court filings, as to all other matters.

## SUMMARY OF THE ACTION

1. This is a shareholder derivative action arising out of a reckless, self-interested scheme by the Individual Defendants and T-Mobile's largest stockholder—Deutsche Telekom ("DT")—that has harmed and continues to harm T-Mobile shareholders in order to serve DT's own interest.

2. Beginning in 2018 after DT struck a deal with SoftBank to create the United States' second-largest pool of wireless subscribers in a single entity, DT pressed upon T-Mobile a reckless plan to hurriedly create a broad data-mining architecture that could allow the new T-Mobile to contribute to DT's groupwide machine learning and artificial intelligence apparatus.

3. Specifically, between 2013 and 2017, DT and its T-Labs division had devised a sweeping data- and model-sharing plan to aggressively monetize user data and implement AI across DT's many subsidiaries and lines of business. DT's plan—unprecedented in the staid telecommunications space—was to roll out a unified, incredibly audacious data-mining and AI-training architecture across DT's directly controlled "NatCos" and other subsidiaries, such that all components of DT's vast holdings would collectively and cooperatively contribute to DT's data-mining and AI goals. DT data scientists called this the "Sharing is Caring" plan.

4. And by early 2018, it was in full effect. DT had rolled out a "uniform data model" and a so-called "app store for data models" NatCo by NatCo, and subsidiary by subsidiary. Becoming an AI-driven enterprise was a top goal on its forthcoming 2019 Annual Report.

5. However, one component of DT's vast empire was not contributing. T-Mobile was in fact years behind its direct competitors, including AT&T and Verizon, in machine learning and AI as 2018 rolled around. And worse yet, T-Mobile was about to get much, much bigger, as DT reached an agreement with SoftBank in April 2018 to combine T-Mobile and Sprint, with DT retaining majority Board control of the merged entity (and taking on approximately $38 billion in Sprint's debt).

6. DT needed T-Mobile to start contributing to its AI ambitions—especially given that T-Mobile was soon to be one of the single largest sources and repositories of wireless user data in the entire world.

7. In 2018, T-Mobile finally complied. By late 2018, T-Mobile had begun in earnest an aggressive and reckless plan of data- and credential-centralization in order to train machine learning/AI models as quickly as possible, companywide, using as much data as could possibly be made available. The T-Mobile blueprint for this effort was taken directly from DT's T-Labs division—right down to a "Sharing is Caring" principle by which data sources and personnel across the entire T-Mobile organization could access essentially the entirety of the company's historical data with minimal hurdles, in order to prioritize training of AI models over any other concern.

8. T-Mobile even went so far as to centralize the credentials for its disparate databases and repositories—the better to remotely and repeatedly access wide, deep swaths of up-to-the minute customer (and indeed, *non-customer*) data.

9. Although this aggressive data- and credential-centralization apparatus was exactly what DT had devised in-house in the years prior, and served DT's ultimate goal of milking T-Mobile's vast trove of user data to contribute to DT's data-mining and AI ambitions, its execution by T-Mobile and the direction of the Individual Defendants was a disaster for customers. Between late 2018 and late

2021, T-Mobile suffered six major data breaches, including major breaches in November 2019, March 2020, December 2020, February 2021, and August 2021. Throughout this period, customers, regulators, and shareholders watched in amazement as T-Mobile appeared incapable of securing its customer data, despite data breach, after data breach, after data breach.

10. The truth, however, was that T-Mobile ***was*** incapable of securing its customer data from 2018 on—but not because of any technical glitch or malady. Rather, the very data and credential centralization that was causing breach after breach after breach—and indeed, persists to this day, continuing to imperil T-Mobile customer data—was the result of a conscious design decision by T-Mobile at the direction of its captured board and management, one foisted upon it by its DT overlords.

11. Specifically, DT had avowedly adopted an AI-first, data-hungry corporate strategy, and beginning in 2018 T-Mobile was forced to get in line. In order to train the sophisticated AI and machine learning models T-Mobile needed to keep up with and contribute to DT, T-Mobile pooled all its data, pooled credentials, and prioritized (and still prioritizes) model training and accessibility over data security.

12. The results have been predictable—but have cost T-Mobile itself hundreds of millions of dollars, with future liabilities uncertain (as T-Mobile's data

and credential centralization has not been fixed). Just last month, in July 2022, T-Mobile agreed to pay $500 million to settle liabilities from a single data breach, in August 2021.

13. T-Mobile's data centralization frolic and detour has cost its shareholders hundreds of millions of dollars, and imperils the future of an otherwise thriving telecommunications company. However, throughout the period since T-Mobile began aggressively training AI for the benefit of DT, as company's customers suffered high-profile data breach after high-profile data breach, T-Mobile's Board has done nothing to fix the problem. Indeed, T-Mobile's directors and top executives have continued to centralize data and credentials year-in and year-out, and have indeed paid out giant sums of company money to continue business as usual.

14. The reason that no one within T-Mobile has stepped up to fix the problem—including T-Mobile's Board, which has a fiduciary duty to protect T-Mobile from the avarices of a single shareholder—is because that single shareholder has compromised a majority of the Board, and the Company's top executives, throughout the period of time covered in this Complaint.

15. Since 2013, DT has controlled a majority of the seats on T-Mobile's Board. At present, six members of T-Mobile's 13-member Board (including T-Mobile's Chairman) are current DT executives and/or Board members; another

member of T-Mobile's Board owns approximately $750 million in stock currently subject to a DT-controlled lock-up and proxy agreement; and another T-Mobile Board member is Michael Sievert, the T-Mobile CEO who has presided over the whole data aggregation mess since 2019.

16. T-Mobile's directors and officers, as alleged in this Complaint, have breached their fiduciary duties toward the Company, and they have done it in service of their true master: DT. This shareholder derivative action seeks appropriate damages and injunctive relief to remedy the harm these directors have caused to the company and its stockholders, including Plaintiff.

## PARTIES

### A. Plaintiff

17. Plaintiff Jenna Harper is a stockholder of T-Mobile and has been a continuous stockholder at all times relevant to the claims asserted here.

### B. Nominal Defendant

18. Nominal Defendant T-Mobile US, Inc., is a Bellevue, Washington-based corporation incorporated under the laws of Delaware. T-Mobile's headquarters is located at 12920 SE 38th Street, Bellevue, WA 98006.

19. T-Mobile is a telecommunications company that, among other things, provides mobile and wireless services to approximately 102.1 million customers in the United States. T-Mobile, through its two flagship brands T-Mobile and Metro by

T-Mobile, provides service, devices, and accessories through its owned and operated retail stores, its online store, and T-Mobile apps for mobile devices and smartphones.

20. T-Mobile's Fifth Amended and Restated Certificate of Incorporation states that the Court of Chancery of the State of Delaware shall be the sole and exclusive forum for any derivative action or proceeding brought on behalf of the Company.

### C. Director Defendants

21. Defendants Sievert, Höttges, Claure, Datar, Illek, Kübler, Long, Langheim, Leroy, Taylor, Tazi, Westbrook, and Holloway comprise the T-Mobile Board of Directors. As established below, demand is excused as to each of the Director Defendants.

22. Defendant Michael Sievert is the President and CEO of T-Mobile. He has served as a T-Mobile Board member since 2018. He previously served as T-Mobile's COO from 2015 to 2018 and as President and COO from 2018 to 2020. Sievert has worked at T-Mobile since November 2012. Since 2018, Sievert has received over $100 million in total compensation from T-Mobile in the form of salary, bonus, stock awards, non-equity plan compensation, and other compensation. Sievert was President and/or CEO of T-Mobile throughout the entire scheme alleged in this Complaint.

23. Defendant Timotheus Höttges is the Chairman of T-Mobile's Board. He has served as a T-Mobile Board member since 2013. Höttges is the Chair of the T-Mobile Board's Executive Committee and Selection Committee. Höttges is also the CEO of DT, T-Mobile's largest and controlling shareholder. Höttges has served several different roles at DT since 2006, including as CFO from 2009 to 2013.

24. Defendant Christian Illek has served as a T-Mobile Board member since 2018. Illek is the Chair of the T-Mobile Board's Compensation Committee. Illek is also a member of the T-Mobile Board's Executive Committee and CEO Selection Committee. Illek has been the CFO of DT, T-Mobile's largest and controlling shareholder, since 2019. Illek has been on the DT Board since 2015.

25. Defendant Raphael Kübler has served as a T-Mobile Board member since 2013. Kübler is a member of the T-Mobile Board's Compensation Committee and Executive Committee. Kübler has been a Senior Vice President at DT, T-Mobile's largest and controlling shareholder, since 2014. Kübler has served in numerous other roles at DT and/or DT subsidiaries since 2003.

26. Defendant Thorsten Langheim has served as a T-Mobile Board member since 2013. Langheim is a member of the T-Mobile Board's Compensation Committee, Executive Committee, and Selection Committee. Langheim is on the Board of DT, T-Mobile's largest and controlling shareholder. Langheim has worked at DT since 2009 in a variety of executive roles; he is currently Chairman and Co-

Founder of Deutsche Telekom Capital Partners, the venture capital and private equity arm of DT.

27. Defendant Dominique Leroy has served as a T-Mobile Board member since 2020. Leroy is a member of the T-Mobile Board's Nominating and Corporate Governance Committee. Leroy is on the Board of DT, T-Mobile's largest and controlling shareholder.

28. Defendant Omar Tazi has served as a T-Mobile Board member since 2020. Tazi is a Senior Vice President at DT, T-Mobile's largest and controlling shareholder, where Tazi focuses on technology and big data, including AI.

29. Defendant Marcelo Claure has served as a T-Mobile Board Member since 2020. Claure is a member of the T-Mobile Board's Compensation Committee, CEO Selection Committee, and Executive Committee. Until early 2022, Claure also served as the CEO of Softbank International and COO of Softbank. Claure is the beneficial owner, through Claure Mobile LLC, of 7,034,791 shares of T-Mobile stock. At least 5,000,000 of these shares (worth more than $750 million on the open market as of the date of this Complaint) are subject to a proxy and lockup agreement with DT that, among other things, prevents Claure from selling his shares without DT's authorization.

30. Defendant Kelvin Westbrook has served as a T-Mobile Board member since 2013. Westbrook is the Chair of the T-Mobile Board's Compensation

Committee. Westbrook also serves as a member of the T-Mobile Board's Audit Committee. Westbrook owns 27,692 shares of T-Mobile stock. Westbrook has received over $1.5 million in compensation from T-Mobile since 2018, including $735,889 in 2020.

31. Defendant Srikant Datar has served as a T-Mobile Board member since 2013. Datar is the Chair of the T-Mobile Board's Audit Committee. Datar owns 35,767 shares of T-Mobile Stock. He has received over $1.5 million in compensation from T-Mobile since 2018, including $759,183 in 2020

32. Defendant Bavan Holloway has served as a T-Mobile Board member since 2021.

33. Defendant Teresa Taylor has served as a T-Mobile Board member since 2013. Taylor is the Chair of the T-Mobile Board's Nominating and Corporate Governance Committee. Taylor also serves as a member of the T-Mobile Board's Audit Committee and CEO Selection Committee. Taylor has been designated by the T-Mobile Board as its lead independent director. Taylor has received over $1.5 million in compensation from T-Mobile since 2018, including $767,575 in 2020.

34. Defendant Letitia Long has served as a T-Mobile Board member since 2021. Long is a member of the T-Mobile Board's Nominating and Corporate Governance Committee. Long also serves as T-Mobile's National Security Director. Long previously served as the Director of the National Geospatial-Intelligence

Agency and has nearly four decades of experience in the security and intelligence industry.

### D. Former Director Defendants

35. Defendant Michael Wilkens served as a T-Mobile Board member between November 2020 and June 2022. Westbrook was a member of the T-Mobile Board's Compensation Committee. While Wilkens was on T-Mobile's Board, he was a Senior Vice President at DT, T-Mobile's largest and controlling shareholder. Wilkens served in numerous other roles at DT or DT subsidiaries since 2001. In April 2022 T-Mobile announced that Wilkens would not be standing for reelection "in connection with his planned departure from Deutsche Telekom AG."

36. Defendant Srini Golapan served as a T-Mobile director from 2019 to late 2020. During his tenure on the T-Mobile Board, Golapan was a DT executive and a member of DT's Board of Management.

37. Defendant Lawrence H. Guffey served as a T-Mobile director from 2013 to mid-2021. Guffey was a member of the Supervisory Board at DT prior to joining the T-Mobile board.

38. Defendant Ronald D. Fisher served as a T-Mobile director from mid-to-late 2020, during which time he was an executive at SoftBank.

### E. Officer Defendants

39. Defendant Michael Sievert is also sued in his capacity as a T-Mobile officer—to wit, as the Company's CEO since 2020, and prior to that its President and COO since 2018.

## FACTUAL BACKGROUND

## II. THE WIRELESS INDUSTRY EMBRACES AI

40. In late 2017 and early 2018, mobile carriers began an overhaul of their complex computer systems. Large carriers, like T-Mobile's then-competitors AT&T, Sprint, and Verizon, rushed to convert their legacy, monolithic computer systems into microservices, which are smaller, special-purpose pieces of software.

41. The reason mobile carriers rushed to make this overhaul—which represented a significant departure from long-established hardware and software paradigms at AT&T, Sprint, and Verizon—was that a conversion to microservices allowed these companies, which once had to maintain their own vast data centers, to deploy the systems and software that form the core of their businesses (from customer support, to e-commerce, to marketing, to back office functions like logistics and accounting) on cloud computing systems. For mobile carriers AT&T, Sprint, and Verizon, converting legacy computing systems to microservices in the cloud would permit these data-centric companies to access massively scalable, on-demand computing power for their operations.

42. And not just any sort of computing power. The computing power that was suddenly available to AT&T, Sprint, and Verizon with their abrupt move to the cloud included special-purpose hardware arrays designed to process vectors of information. These Graphics Processing Units ("GPUs")—purpose-built to process large blocks of data in parallel—were historically used in graphics processing systems and gaming systems.

43. These same processors, could, however be used to perform a new class of algorithms designed to learn directly from large amounts of data. Software embodying these algorithms, which is sometimes referred to as machine learning ("ML") or even artificial intelligence ("AI") software, does not require a programmer to write a priori instructions for computer programs to make complex decisions.

44. Instead, machine learning algorithms allow for computational decision-making based on inferences from data. The processing power required to run machine learning algorithms on large quantities of data at scale is immense—a power never before seen in the private sector until the past half-decade, when rapid developments in cloud computing made entire data centers of rapidly scalable GPU arrays commercially available to data-centric businesses like mobile carriers.

45. By late 2017 and early 2018, deploying (or re-deploying) a company's computing infrastructure and systems in the cloud meant that the company could

build connected systems that learned directly—and constantly—from customer data. For businesses like mobile carriers—which store, collect, and process mass quantities of data from millions of subscribers and billions of unique data sources every second of every day—moving companywide computing infrastructure to the cloud meant the prospect of using algorithmically-gleaned insights and decisions to rapidly outperform legacy competitors on customer acquisition, retention, and other key metrics.

46. By early 2018, each of T-Mobile's then-principal competitors—Sprint, AT&T, and Verizon—had recognized the potential of this new technology to their business and were already beginning to use cloud-based machine learning/artificial intelligence software to monetize customer data at scale.

47. For example, Sprint—then owned by Japanese conglomerate SoftBank—announced in March of 2018 that it would use AI to power its call centers. The Wall Street Journal reported on the announcement:

> Sprint Corp.'s technology executives say they're working to develop AI-powered software that could help call center representatives with customer inquiries, in an example of how artificial intelligence is poised to work alongside the human workforce.
>
> The effort is part of Sprint's ongoing digital transformation project, which involves a partnership with Adobe Systems Inc. and an emphasis on delivering value from big data and analytics.

48. The new approach, however, could only work if the company leveraged massive amounts of its customers' data. As the Wall Street Journal further reported, Sprint's Chief Information Officer, Scott Rice, made clear the company's plans to heavily leverage customer data to build AI-based applications:

> Mr. Rice said the company is planning on using massive amounts of data about customer calls to develop so-called "interaction assistants," or software programs that can suggest the next best steps for employees to take during a call. The software would be powered by machine learning, a subfield of artificial intelligence that enables computers to learn from data with minimal programming.
>
> For example, if a call center employee is talking to a customer about a specific topic, the company could use machine learning to turn the audio into text, analyze it, and return filtered results to give them real-time potential solutions to help that customer, said Rob Roy, Sprint's chief digital officer. Mr. Roy is working alongside Mr. Rice on the digital transformation initiative.

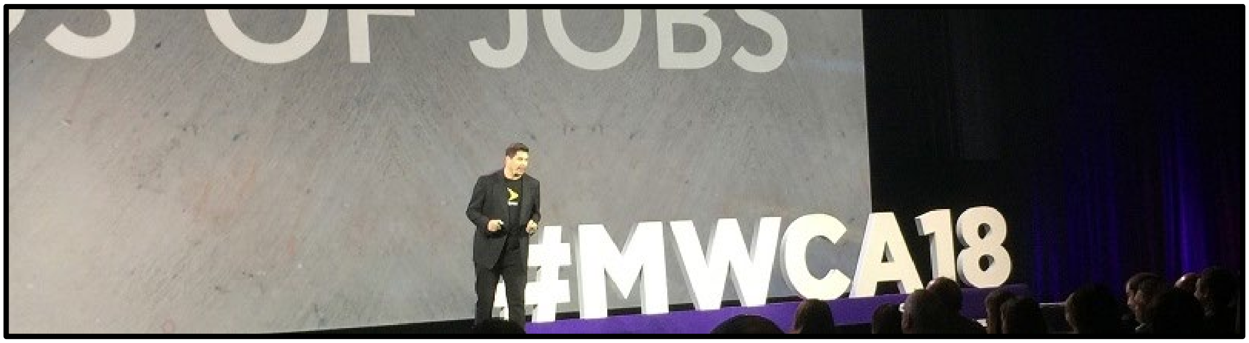
49. Sprint was not, however, simply planning to use AI to assist with customer service. It was going to use it to give it an edge over its competitors in marketing:

> Sprint's technology executives say they're also using data as a way to customize digital marketing advertisements to specific customers. Using an Adobe service that collates anonymized IP address data, Sprint can tell whether two devices—for example, a mobile phone and a laptop—are connected to a current or prospective customer.
>
> That way, if a person is browsing a specific product on their mobile phone, a personalized message could pop up on that same person's desktop about that same product.

> "The more tailored we can be in our messaging, it'll help us reduce churn and improve customer satisfaction," Mr. Rice said. ". . . In such a competitive wireless and telecommunications environment, what it comes down to is raising the level of service, communication and interaction with that customer base."
>
> For about six months the company has been using so-called cross-device identification to help target digital advertisements. Sprint's technology executives declined to disclose details on how it's impacted the business.
>
> "It's been extremely beneficial to us in how we think about and use our data to create better decisions," Mr. Roy said.

50. By mid-2018, it was clear that customer information was being mined for a competitive edge among wireless carriers. It was the beginning of an AI- and data-driven arms race.

51. In September 2018, Sprint's then-Chairman Marcelo Claure—until January 2022 the COO of SoftBank, and a current T-Mobile Board member—took the stage at a conference in Los Angeles in and told the audience that companies that embraced AI along with 5G networks "are always going to win."



52. Claure—the SoftBank executive and T-Mobile board member—likened the transition to AI to the cultural transition from horse-drawn carriages to automobiles. The future meant rapidly moving to AI-based systems, not procedurally-written computer programs created by large teams of software developers hardcoding software decisions.

53. Similarly, in an interview in August 2018, AT&T's Vice President of Technology, Shared Platforms & Engineering, Paul Fox, proclaimed that AI would allow AT&T to "hyper-automate" across its business.

54. AT&T was ahead of the curve, having deployed thousands of machine learning and AI driven "software robots" throughout its organization. That software was deployed on cloud-based servers, where AT&T would have access to arrays of GPUs optimized for AI-based computation.

55. Quoting AT&T's Chief Data Officer Steve Stine in February 2018, the Wall Street Journal reported that AT&T had made widespread headway within its company with its AI efforts:

> AT&T's data optimization efforts, which include software robots, advanced analytics and artificial intelligence, have helped generate hundreds of millions of dollars worth of business value in recent years, Mr. Stine said. Bots have processed millions of minutes of work and they've saved employees from significant amounts of mundane work over the past two years, he said.

56. In fact, AT&T's data and AI push began well before Sprint's—in 2015. By 2016, the company had launched an online training program to teach its employees how to build AI and machine learning bots. By 2018, AT&T had 2,000 employees across 100 different organizations trained to build such systems.

57. The bottleneck for AT&T, however, was not the number of people it trained. The bottleneck was customer data, including the task of cleaning and structuring data so that it could be consumed by AT&T's machine learning- and AI-based applications and models. Yet even that task, AT&T was starting to automate by 2018.

58. And by 2018 Verizon, too, was leveraging AI across its business—for example, by deploying AI tools to monitor the quality of service across Verizon's broadband and wireless networks. Whereas the company had previously relied on customer feedback to determine whether (and where) there were problems in its network, Verizon had now built and deployed AI that directly learned from, and monitored, usage data.

59. Verizon's Executive Vice President had already announced the company's commitment to AI in August 2017. Like Sprint, Verizon was using customer data to market products to customers and potential customers. For example, Verizon was using customer data to create a "rewards" program that segmented its user base, allowing it to target specific products to categories of users.

60. By the end of 2018, each of T-Mobile's then-chief competitors was deploying AI and ML tools in the cloud to analyze, learn from, and improve business outcomes from customer data in real-time. And the technology to algorithmically process mass data at scale was only accelerating in its availability and applications. For the data-centric—and fiercely competitive—mobile industry, the potential competitive edge from cloud-based ML/AI insights gleaned in real-time from customer data had become a drumbeat that no major carrier could ignore. Except for years, T-Mobile had done just that.

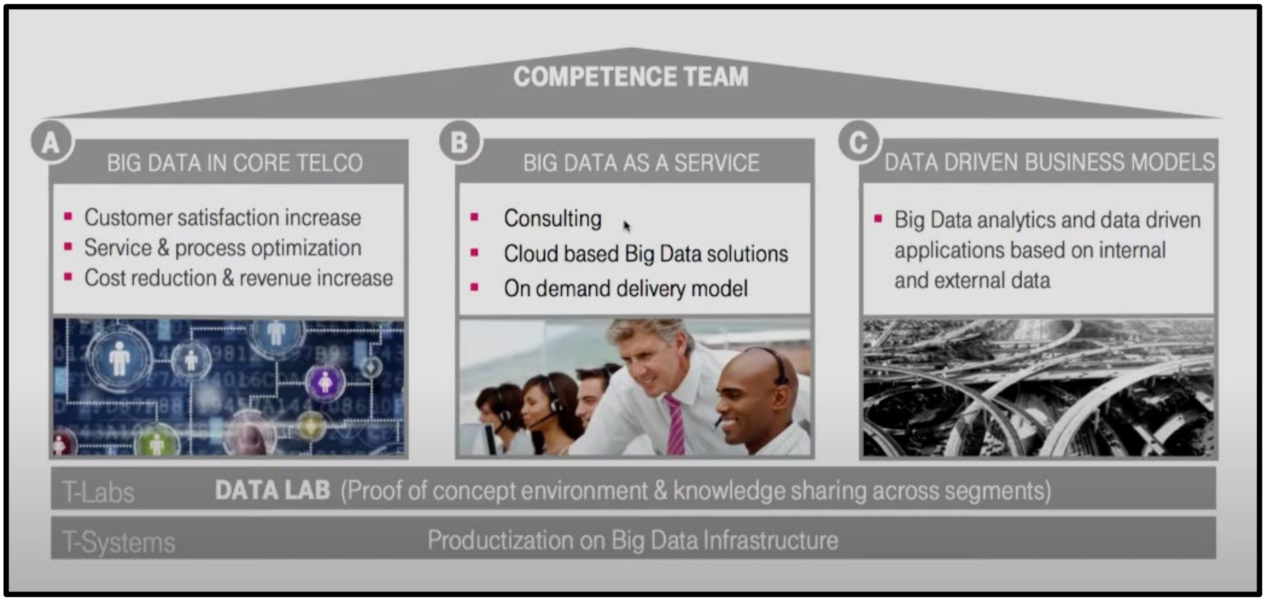
## III. DEUTSCHE TELEKOM'S AGGRESSIVE AI PUSH AT ITS DIRECT-CONTROL SUBSIDIARIES AND AFFILIATES

61. By contrast, in Germany, Deutsche Telekom—the largest telecommunications provider in Europe by revenue, with owned-or-controlled subsidiaries (referred to by DT as its "NatCos") in Austria, Bosnia and Herzegovina, Croatia, Czech Republic, Germany, Greece, Hungary, Montenegro, North Macedonia, Poland, Romania, and Slovakia—took early notice of the prevailing industry winds.

62. In 2014, a small team within DT's Telekom Innovation Laboratories (T-Labs) subgroup—led by DT Vice President Susan Wegner, a Ph.D. data scientist—was asked to research ways in which DT might benefit from Big Data, including through the adoption of "Data Driven Business Models." Wegner's team

worked as a "Data Lab," developing a proof-of-concept environment and knowledge-sharing across DT's vast business segments.

63. The team's initial mandate was wholly theoretical, and it included an evaluation of legacy "Core Telco" uses of DT's and its subsidiaries' customer data. As Wegner later explained it in an August 2016 presentation, her team had "three topics" to look into (1) Big Data in Core Telco, (2) Big Data as a Service, and (3) Data Driven Business Models:



COMPETENCE TEAM

A BIG DATA IN CORE TELCO

- Customer satisfaction increase
- Service & process optimization
- Cost reduction & revenue increase

B BIG DATA AS A SERVICE

- Consulting
- Cloud based Big Data solutions
- On demand delivery model

C DATA DRIVEN BUSINESS MODELS

- Big Data analytics and data driven applications based on internal and external data

T-Labs **DATA LAB** (Proof of concept environment & knowledge sharing across segments)

T-Systems Productization on Big Data Infrastructure

64. Of these topics, the third—Data Driven Business Models—was the one that most interested Wegner, the data scientist. It was, as Wegner later recounted, "very disruptive" and represented a change to the entire landscape of how DT viewed its business.

65. As Wegner explained, by 2013-14, there were giant companies—principally in Big Tech—whose entire business model was based on the aggressive

acquisition, aggregation, analysis, and monetization of user data. Her team thought, why not DT?

> So . . . we sat together as a team and we thought okay, we have the Google, Facebook, and everything out there—so what do we have at Deutsche Telekom? So we thought okay one use [would] be, is the data. And then we thought, what can we do with the data?

66. The answers Wegner's team came up with about "what [DT] c[ould] do with the data" would change the course of DT's company-wide strategy, structure, and corporate mission—and would eventually be hurriedly foisted upon its partly-owned affiliate T-Mobile in conjunction with a Sprint merger that brought AI-forward parent Softbank into that company.

67. Wegner's team found that there was demand—indeed, transformational demand—for data-driven solutions across "every department" at DT. As Wegner explained in 2016, her team was at that time getting requests for analytics- and data-driven applications "every hour" from across the business, and noted that DT's CFO and its Board both sought her team's expertise for organization-wide strategy.

68. The problem, however—the "major hurdle," as Wegner described it in 2016, was DT's legacy data systems, which were set up to securely store and selectively access data, not to comingle and mine it:

> [T]he major hurdle here is really to get access to the data because we have a lot of data in the systems but when the systems were set up you don't have the APIs to get the

> data out of the systems, so we are struggling a little bit here
> with that one.

69. Additionally, some of the specific use cases Wegner's group proposed for DT's customer data ran into high-level pushback due to privacy concerns. For example, early on, Wegner's team proposed that DT combine its customers' real-time location data with other subscriber data to power use cases "like real-time knowing how many people are in a bus, how many people are in a train so you can inform the customer this train's full, wait for the next one," or "for emergency cases . . . more or less having heat maps of people."

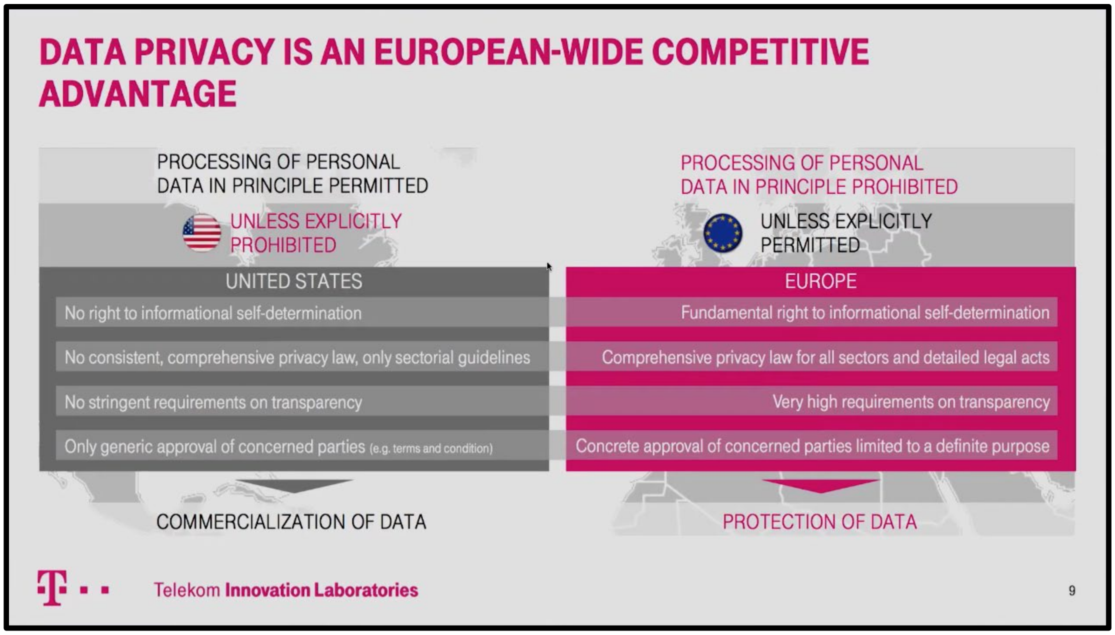
70. According to Wegner, "that might not be so disruptive in other countries, but we are very sensitive concerning privacy within Germany," such that Wegner "had to go into the board [at Deutsche Telekom] and we had to convince for example our communication guy, I remember the first meeting with him was like ice . . . ."

71. Eventually, DT's board was swayed—although only partially. Wegner's proposals were very intriguing to DT's highest decisionmakers, but the problem remained of Germany's uniquely restrictive privacy laws, and the fact that DT was leery of Wegner's aggressive data-mining work being conducted under its own name. As Wegner explained it, "as you can imagine, this is not a topic which you can develop within a large company, that's the reason why we set up our own

company for that one three years ago and as a hundred percent subsidiary of Deutsche Telekom . . . .”

72. By late 2016, Wegner’s group was continually working to provide data-driven solutions to DT’s highest-level executives, and indeed, its board. But a key problem remained: in order to effectively develop and use high-end, data-driven models and solutions at DT, data from across the entire business had to be easily accessible to teams across the company—and much of DT’s data and systems had never been designed for that. Moreover, Wegner’s group faced a real problem of privacy arbitrage, especially throughout Europe, which made it complicated to commingle data from its different NatCos and other subsidiaries and affiliates.

73. As Wegner explained it, her group didn’t know much about data privacy except that “in Europe and especially in Germany you do everything to protect the data” whereas “in the U.S. you really have more focus on how you can commercialize your data.” The below slide summarized DT’s thoughts, sourced from a DT “board member”:



DATA PRIVACY IS AN EUROPEAN-WIDE COMPETITIVE ADVANTAGE

PROCESSING OF PERSONAL DATA IN PRINCIPLE PERMITTED

UNLESS EXPLICITLY PROHIBITED

PROCESSING OF PERSONAL DATA IN PRINCIPLE PROHIBITED

UNLESS EXPLICITLY PERMITTED

| UNITED STATES | EUROPE |
|---|---|
| No right to informational self-determination | Fundamental right to informational self-determination |
| No consistent, comprehensive privacy law, only sectorial guidelines | Comprehensive privacy law for all sectors and detailed legal acts |
| No stringent requirements on transparency | Very high requirements on transparency |
| Only generic approval of concerned parties (e.g. terms and condition) | Concrete approval of concerned parties limited to a definite purpose |

COMMERCIALIZATION OF DATA

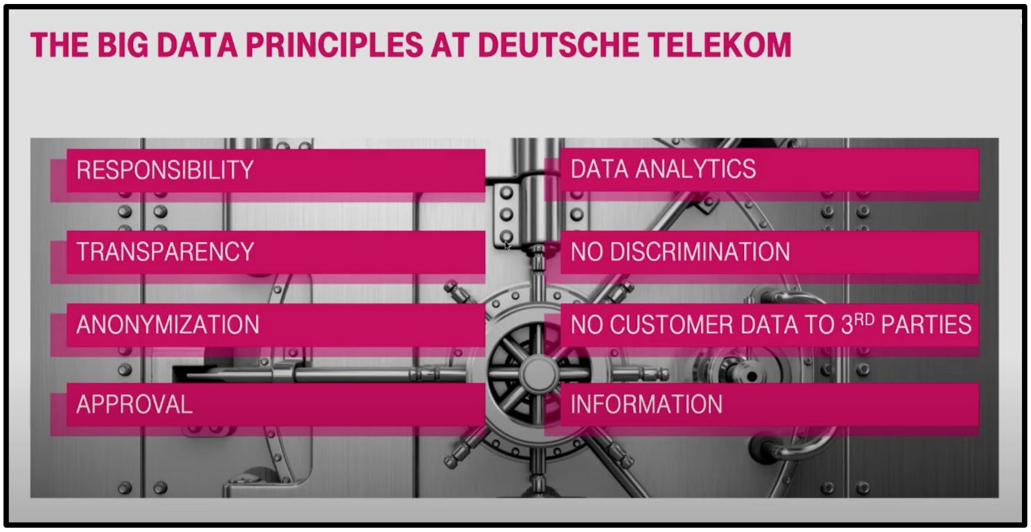
PROTECTION OF DATA

Telekom Innovation Laboratories

9

74. In short, DT learned early on in the AI revolution that one way to get around European data privacy regulations and disclosures was to process data in the United States. The German telecom knew essentially nothing about U.S. privacy law: DT viewed it as the Wild West, and told its engineers and business strategists as much in official, written communications.

75. Besides privacy arbitrage—with the U.S. being the principal location where DT believed it could aggressively co-locate and mine data—DT's nascent AI/ML team also learned another useful strategy to outflank DT's privacy obligations and disclosures, and in particular the company's "Big Data Principle" that customer data was not to be shared with third parties: conglomeration.



THE BIG DATA PRINCIPLES AT DEUTSCHE TELEKOM

RESPONSIBILITY

TRANSPARENCY

ANONYMIZATION

APPROVAL

DATA ANALYTICS

NO DISCRIMINATION

NO CUSTOMER DATA TO 3$^{RD}$ PARTIES

INFORMATION

76. Specifically, DT subsidiaries could act in ways the parent company wouldn’t, yet at the same time customer data from across DT’s subsidiaries and affiliates could be transferred and/or processed without technically using “third parties.”

77. As Wegner explained it:

> We are not giving data to third parties, that’s exactly why we set up Motion Logic [the data-mining venture based on Wegner’s “heat map” proposal] as a one hundred percent subsidiary of Deutsche Telekom . . . .

78. Using the above principles—cross-border privacy arbitrage and conglomeration—DT began in earnest in early to transform its entire business model around data-hungry AI.

79. In April 2017, DT outlined its near-term AI strategy in a lengthy article on its website:

> **At Deutsche Telekom, development of AI systems is an important priority.**

> Instead of buying "off-the-shelf" AI systems and robots, which can be expensive, Deutsche Telekom is developing its own AI solutions—via its developer teams, and with the support of partners. And it is testing AI-based software, computers, voice control functions and chatbots, with a view to making customer service more efficient, for consumers and corporate customers alike. . . .
> Significantly, in the interest of coordinating its efforts in this area, Deutsche Telekom has launched an overarching AI program, eLIZA, for the purpose of linking all AI solutions within the Deutsche Telekom Group.

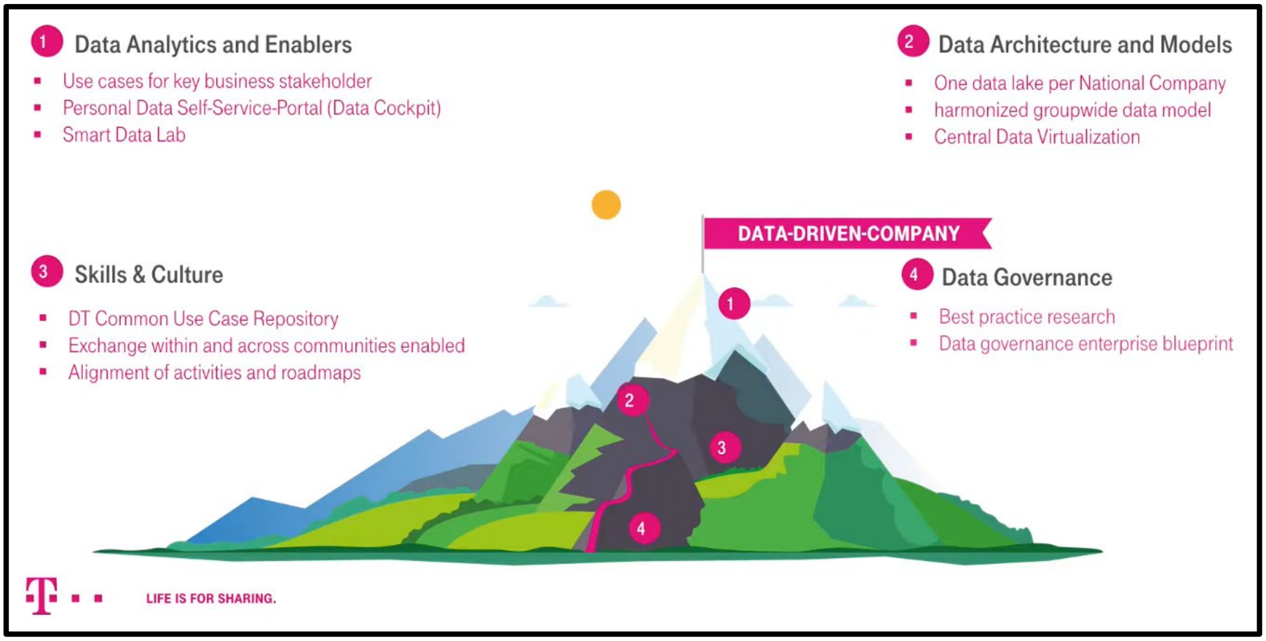
80. DT's article identified several discrete AI projects being developed across its various NatCos and subsidiaries: Tinka, a virtual employee at T-Mobile Austria; Sophie, a service bot and chatbot from DT's subsidiary Congstar; Vanda, an invisible assistant for corporate customers developed by a T-Systems team working in Hungary; and hub:bot, a digital assistant used for recruiting at Hub:raum, DT's startup incubator. But unifying all these discrete AI projects across DT's subsidiaries was eLIZA, which was run by Wegner's old division, T-Labs (Wegner herself had ascended to Vice President Data, Artificial Intelligence, and Governance for all of DT by early 2017). As DT explained:

> **eLIZA: AI for many areas throughout the Group**
>
> The eLIZA program is backed by a team from Deutsche Telekom's Innovation Laboratories (and other innovation areas), as well as by a design team staffed by T-Mobile Austria and Telekom Deutschland.
>
> "In light of the huge sums that players such as Amazon and Google are investing in AI, we feel it makes great

> sense for us to concentrate on using AI in customer service—and, in the longer term, on developing various other areas of interest," explains Jan Hoffman, head of eLIZA. "We want to use AI to solve specific customer problems."
>
> The eLIZA program is to serve as a framework for setting up AI-based systems at various locations throughout the Group, and in various countries. Trinka, Sophie and their virtual colleagues will one day be able to learn from chat logs and from real-time conversations between customer service agents and customers. And they will be able to remember and apply the best ideas, approaches and strategies they cull from these sources.

81. Over the next year, as DT transformed itself into an AI-driven enterprise, Wegner's team developed standardized data models, tools, strategies, and frameworks for information sharing across DT's disparate NatCos and subsidiaries. By 2018, DT was rolling out a standard strategy, developed by Wagner's T-Labs group and intended to increase DT's companywide profits, to each of its NatCos and business units—even those with distinct (*e.g.*, country-specific) data pools.

82. As Wegner explained in July 2018, her T-Labs team was tasked by the DT board with rolling out a "harmonized groupwide data model" across all of DT's NatCos and subsidiaries, and developing "Central Data Virtualization" across all of DT's component companies:



1 Data Analytics and Enablers

- Use cases for key business stakeholder
- Personal Data Self-Service-Portal (Data Cockpit)
- Smart Data Lab

2 Data Architecture and Models

- One data lake per National Company
- harmonized groupwide data model
- Central Data Virtualization

3 Skills & Culture

- DT Common Use Case Repository
- Exchange within and across communities enabled
- Alignment of activities and roadmaps

4 Data Governance

- Best practice research
- Data governance enterprise blueprint

LIFE IS FOR SHARING.

83. This entailed, among other things, developing alignment of activities and roadmaps across DT's various NatCos and subsidiaries, creating a DT Common Use Case Repository for data mining and AI/ML tools and in fact models, and facilitating exchange within and across communities within DT's many companies and subgroups.

84. Each National Company within DT was to have its own distinct "data lake"—a pooled, centralized repository of all data available to that NatCo, open to mining by ML/AI tools and other data tools from across the company—and then commingle and share everything learned from that data, including ML/AI models, for the benefit of DT as a whole. Moreover, each DT NatCo and subsidiary was to follow a harmonized data model and align its ML/AI activities and strategies with

those of the parent—*i.e.*, the data model, activities, and roadmaps developed my Wegner's group for use across all of DT.

85. As Wegner explained:

> So what we are doing is that we are helping our business units to really implement cases within our countries, and what we are doing there is really, harmonized use cases. I will have the example later on to have a deep dive, we have the data architecture and model and that's more the ground because the data engineering part . . . takes normally 80% of the time, so we established already . . . a data model within DT and we proposed a data platform for that. What we have for data governance what we have a data governance blueprint for DT and are now implementing use case by use case in different of our countries, so it's in Germany, in Croatia, in Austria, in . . . Macedonia.

86. Wegner called the reuse, exchange, and DT-wide patterning of data architecture, governance, and access across DT's NatCos and business units the parent company's "sharing is caring" initiative regarding ML/AI and Big Data:

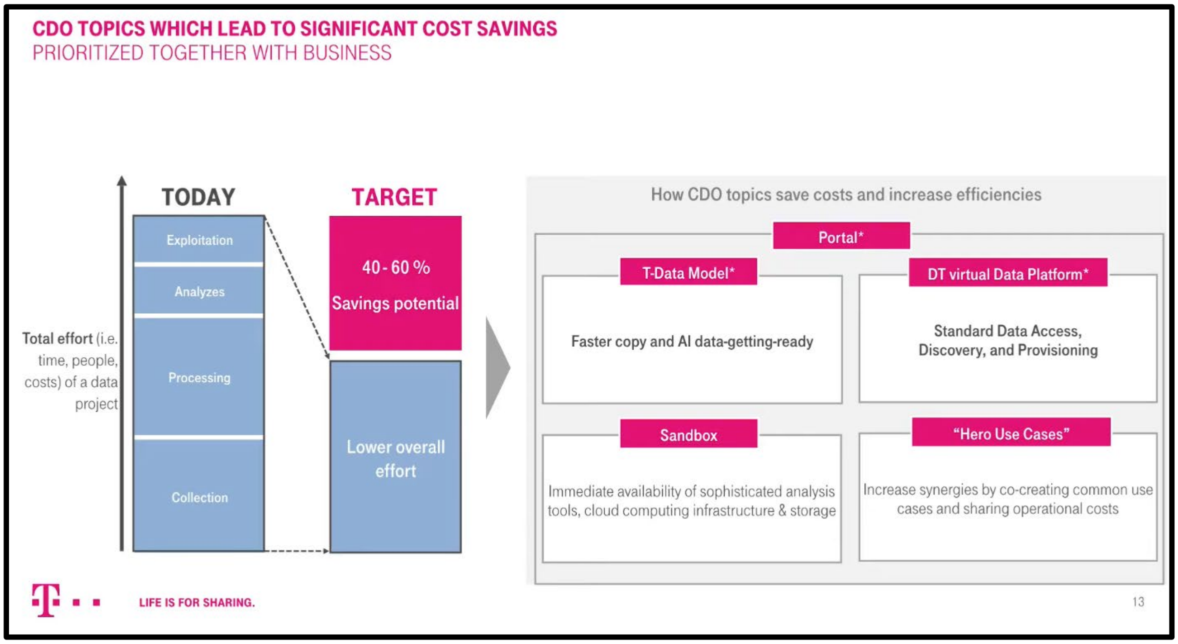
87. The proposition that a company as large as DT—which consists of giant country-specific telecommunications subsidiaries across the globe, as well as giant enterprise and research business units—would take a "sharing is caring" approach to data exchange and model training surprised a participant in Wegner's talk, leading to this exchange:

> EMCEE: Now, it's quite unusual for a company as big as Deutsche Telekom, right? Because normally in big companies it's like my department versus your department, sharing is not exactly the heart of the whole company experience, right?
>
> WEGNER: Yeah, but if you see if we want to really go deeper into artificial intelligence, this is an enabling topic—like, data is an enabling topic. You can only really scale if you share information because if you have it only in one department you will have some cases but you wouldn't have such a big business impact as—than if you really have sharing it all over the company. And that sharing means data sharing, tool sharing, model sharing, and business experience sharing.

88. Wegner emphasized the "business impact" for DT of standardizing and sharing common data, common tools, common models, and common data-driven business strategies and roadmaps across DT's many NatCos and business units, explaining:

> The main thing here is really about the savings. So we started . . . with a common data model, to have one model within DT to look at how we access data, how we have data privacy in there, we have [a] sandbox environment with tools and stuff like that, and as you can imagine, we have a priority list, which are our biggest use cases. From

> the status where we are right now, we are not in everything in the end, we are just starting, we already have a saving there of 40%—our estimation is that we will have 60% if we have only these things already implemented.



**CDO TOPICS WHICH LEAD TO SIGNIFICANT COST SAVINGS**
PRIORITIZED TOGETHER WITH BUSINESS

TODAY

Exploitation

Analyzes

Processing

Collection

Total effort (i.e. time, people, costs) of a data project

TARGET

40 - 60 %
Savings potential

Lower overall effort

How CDO topics save costs and increase efficiencies

Portal*

T-Data Model*
Faster copy and AI data-getting-ready

DT virtual Data Platform*
Standard Data Access, Discovery, and Provisioning

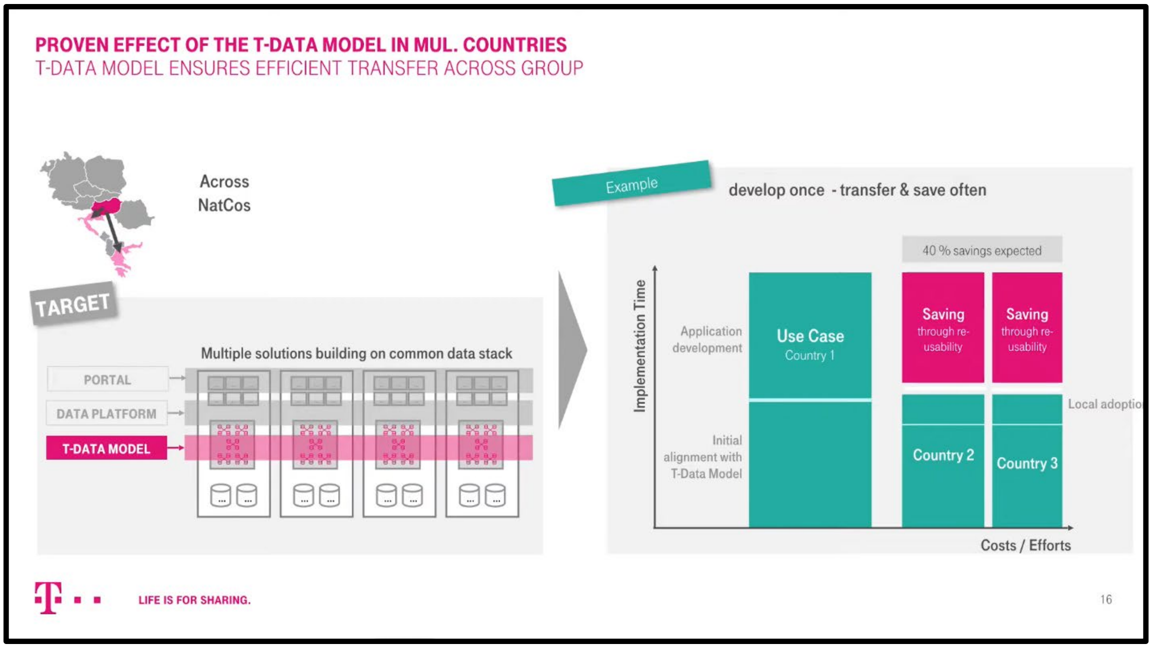
Sandbox
Immediate availability of sophisticated analysis tools, cloud computing infrastructure & storage

"Hero Use Cases"
Increase synergies by co-creating common use cases and sharing operational costs

LIFE IS FOR SHARING.

13

89. Wegner explained that DT was implementing a common ML/AI data model, virtual data platform, and portal across its various NatCos and subsidiaries, country-by-country, in order to save money for the corporate parent:



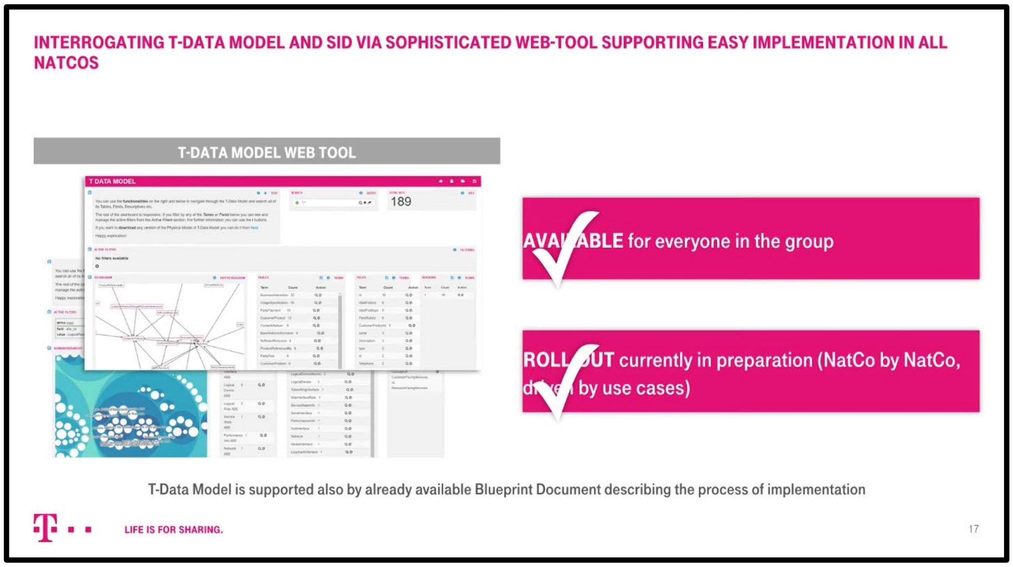
PROVEN EFFECT OF THE T-DATA MODEL IN MUL. COUNTRIES

T-DATA MODEL ENSURES EFFICIENT TRANSFER ACROSS GROUP

LIFE IS FOR SHARING.

16

90. The DT-wide standardization and data-sharing effort was, as of July 2018, to be accomplished through common AI/ML models, strategic blueprints, and tools, standardized and centralized for "easy implementation in all NatCos," "AVAILABLE for everyone in the [DT] group," with a "ROLLOUT currently in preparation (NatCo by NatCo, driven by use cases)":



INTERROGATING T-DATA MODEL AND SID VIA SOPHISTICATED WEB-TOOL SUPPORTING EASY IMPLEMENTATION IN ALL NATCOS

✓ AVAILABLE for everyone in the group

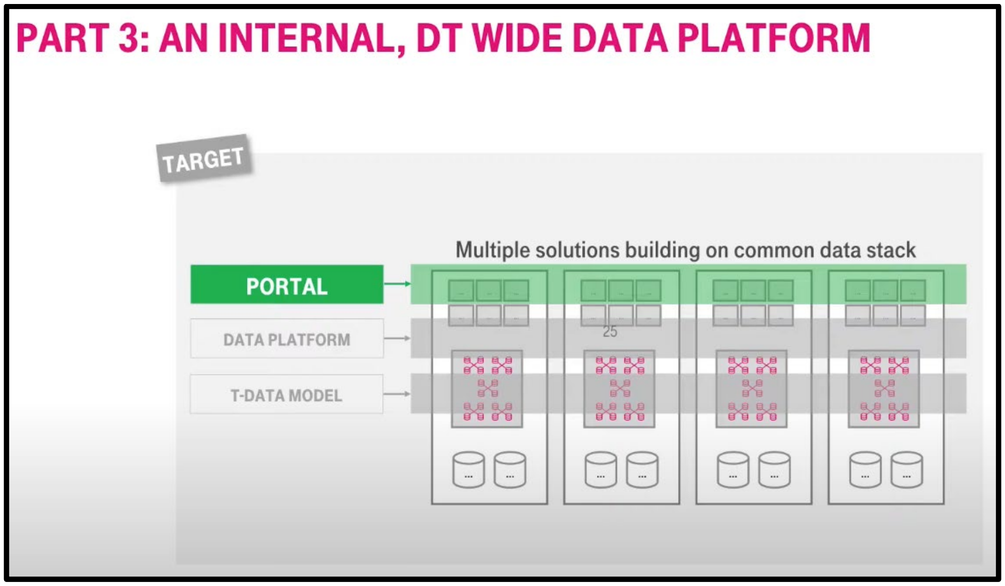
✓ ROLLOUT currently in preparation (NatCo by NatCo, driven by use cases)

T-Data Model is supported also by already available Blueprint Document describing the process of implementation

LIFE IS FOR SHARING.

17

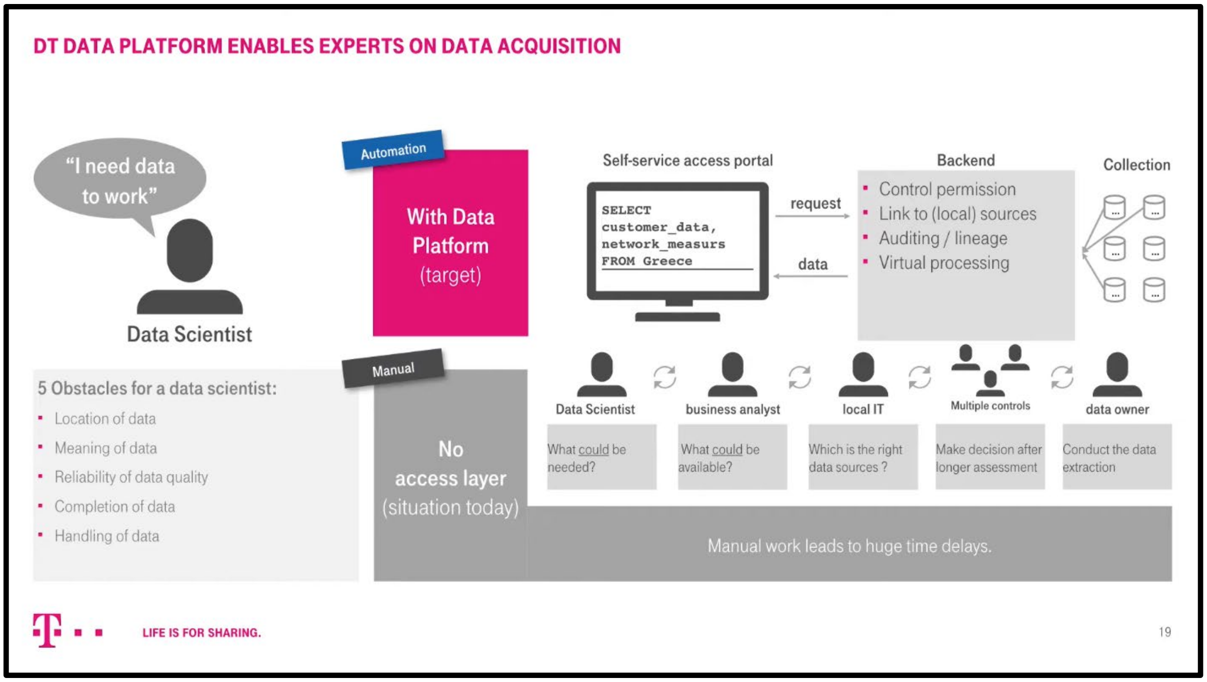
91. But DT wasn't just rolling out common models, blueprints, and tools in 2018—it was also setting up "an internal DT-wide data platform."


PART 3: AN INTERNAL, DT WIDE DATA PLATFORM

92. As Wegner explained:

> And the second one very very briefly it's all about how to access data. So what we experienced in the finance department, it took them six months to really find data for their case, it was a long time because sharing of data was not there . . . . And that's the reason . . . why we said okay we need something like a data platform where we really can access the data all over the company, even though in our different countries we have different kind of implementation of the data lake.

93. And this DT Data Platform wouldn't just centralize models, blueprints, tools, and in fact data, it would incorporate a "backend" that would automatically, in a centralized way, "control permission," "link to (local) sources," and process a request virtually.



DT DATA PLATFORM ENABLES EXPERTS ON DATA ACQUISITION

"I need data to work"

Data Scientist

Automation

With Data Platform (target)

Self-service access portal

```
SELECT
customer_data,
network_measurs
FROM Greece
```

request

data

Backend

- Control permission
- Link to (local) sources
- Auditing / lineage
- Virtual processing

Collection

5 Obstacles for a data scientist:

- Location of data
- Meaning of data
- Reliability of data quality
- Completion of data
- Handling of data

Manual

No access layer (situation today)

| Data Scientist | business analyst | local IT | Multiple controls | data owner |
|---|---|---|---|---|
| What could be needed? | What could be available? | Which is the right data sources ? | Make decision after longer assessment | Conduct the data extraction |

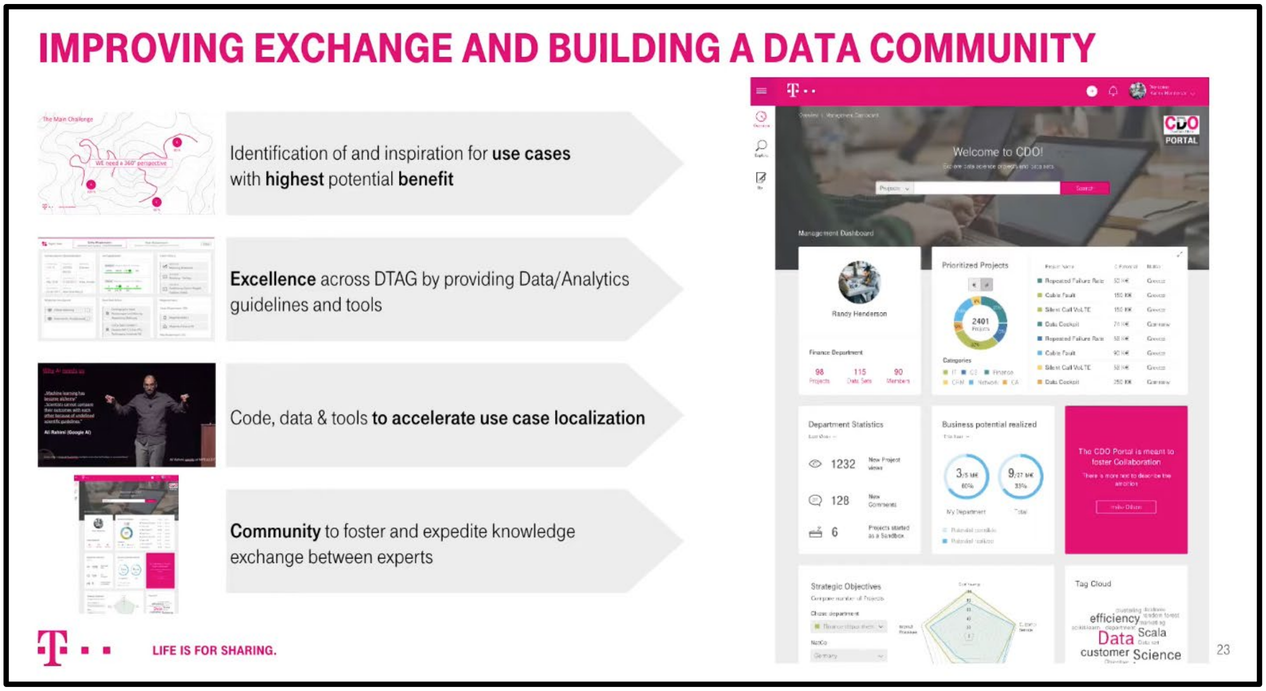
Manual work leads to huge time delays.

LIFE IS FOR SHARING.

19

94. Again, the avowed goal of this DT strategy, which was being rolled out country by country to DT's NatCos and business units in mid-2018, was to improve DT's profitability in data-mining its NatCos and subsidiaries.

95. Moreover, DT was also setting up a centralized, self-service tool for engineers and data scientists across all its NatCos and subsidiaries in which they would place trained models, along with code and comments from data scientists and discussion of business impact, for access across the entirety of DT—what Wegner described as "something like an app store for data models," or her preferred term: "shopping windows."



IMPROVING EXCHANGE AND BUILDING A DATA COMMUNITY

Identification of and inspiration for **use cases** with **highest** potential **benefit**

**Excellence** across DTAG by providing Data/Analytics guidelines and tools

Code, data & tools **to accelerate use case localization**

**Community** to foster and expedite knowledge exchange between experts

LIFE IS FOR SHARING.

23

96. In short, by mid-2018 DT was pushing hard to deploy a uniform—and extremely aggressive—form of data centralization and sharing across its various NatCos and subsidiaries. The reason for this was stated both by Wegner and by DT itself, in its next few Annual Reports: AI. Per Wegner:

> AI is a big topic within DT. Why I'm concentrating on this so much is—I had a team offsite in the morning and it had a slide from our strategy department, and the . . . if you want to go into AI, and I'm talking more about the cognition not about like a metal robot . . . the deep learning is really, you need data and you really need access to the data, you need to have data quality and stuff like that, so for me that's the first step, and that's the reason why we're working on that.

97. As DT explained in its 2019 Annual Report:

> **AI Enterprise:** By integrating artificial intelligence (AI), we will ensure that our products and services remain competitive into the future. For example, AI turns voice

> control, which simply compares entered words against a list of keywords, into a smart assistant. . . . We are working continuously on the convergence of AI and digital processes, and supplying prototypes for a wide range of internal applications.
>
> **Big Data:** In this new innovation area, our focus is on formulating Group-wide principles for data processing and analytics. A uniform data model will enhance our data analyses and enable us to easily transpose successful analyses to new markets. In this context, we ensure that our customer and network data does not leave the country and data network of the corresponding subsidiary.

98. But DT was not the only large, foreign parent of a U.S. telecom looking to increase profits through an aggressive AI/ML strategy in 2017-18.

## IV. SOFTBANK—PARENT OF SPRINT—GOES ALL IN ON AI

99. To Germany's east, another giant conglomerate was going all in on AI—Softbank. And like DT, Softbank also had corporate control over a mid-sized mobile carrier in the United States.

100. In 2012, SoftBank—a giant Japanese conglomerate controlled by founder and CEO Masayoshi Son—spent more than $20 billion to acquire Sprint, America's third-largest wireless carrier behind near-duopolists Verizon and AT&T. Over the next few years, Son publicly sought to acquire T-Mobile, Sprint's four-largest wireless carrier, to create a massive combined entity that could directly take on Verizon and AT&T in the U.S. However, regulatory hurdles—including the

Federal Communications Commission under then-President Barack Obama—stood in Son's way.

101. By 2017, Son's interest—and SoftBank's investments and strategies—had pivoted sharply toward a single subject: artificial intelligence. As the New York Times reported in October 2017:

> When Eric Gundersen, the chief executive of a mapping start-up called Mapbox, met Masayoshi Son, the head of the Japanese conglomerate SoftBank, in late July, he expected to have to sell Mr. Son on what made MapBox important.
>
> But Mr. Son, 60, did not need to be convinced that Mapbox's technology—which powers Lyft drivers and companies like Snap and Mastercard—had value. . . .
>
> What Mr. Son laid out for Mr. Gundersen helps explain why SoftBank and its Vision Fund have invested billions of dollars in a seemingly random sample of more than two dozen companies since the fund was announced. The investments span robotics software start-ups like Brain Corp and the indoor farming business Plenty, as well as more prominent companies like the business software maker Slack. The deals have run the gamut from smaller investments in start-ups to larger deals with public companies.
>
> Yet the companies all have something in common: They are involved in collecting enormous amounts of data, which are crucial for creating the brains for the machines that, in the future, will do more of our jobs and creating tools that allow people to better coexist.

102. A November 2017 Reuters article about SoftBank explained:

> The Japanese tech and telecoms firm is funneling money to U.S. firms as it invests in technology companies around the world, including through its Vision Fund, as founder Son pursues his vision of a future driven by artificial intelligence, interconnected devices and robots.

103. SoftBank's sharp pivot toward AI and data-focused investments in 2017 coincided with DT's similar all-in move toward AI in its own business, including through Wegner's T-Labs group. And it was at this time that DT suddenly realized what a boon T-Mobile's subscribers could be for DT's overall strategic vision. By early 2017, it was DT—T-Mobile's largest shareholder—rather than the United States government that stood in the way of SoftBank's acquisition of T-Mobile. As Fierce Wireless reported in February 2017:

> [S]hares of both T-Mobile and Sprint have risen in recent weeks on speculation that federal regulators will display a lighter regulatory touch under Trump than they did during the Obama administration. And it only increased after Trump announced in December that SoftBank will invest $50 billion in the U.S. in an effort to create 50,000 jobs.
>
> The prospects of such a deal actually occurring are far from clear, however. Deutsche Telekom has indicated it has little interest in spinning off a thriving T-Mobile that has gained tremendous momentum in recent years.

104. By early 2018, it was clear that SoftBank had no interest in T-Mobile—or, indeed, Sprint—beyond those companies' repositories and sources of customer data. As Nikkei Asia reported in March 2018:

> **SoftBank's Son loosens grip on Sprint as passion shifts to AI and robots**

> Five years after buying U.S. telecommunications company Sprint and launching talks with T-Mobile parent Deutsche Telekom to combine the two subsidiaries, SoftBank Group Chairman Masayoshi Son has decided to relinquish control of the carrier he spent nearly $22 billion to acquire.
>
> The decision comes . . . as the Japanese entrepreneur's passions shift from telecommunications to artificial intelligence, the "internet of things" and smart robotics.

105. A March 8, 2018, CNBC article described Son's views on AI at the time:

> People should brace themselves for the proliferation of artificial intelligence as it will change the way we live within three decades, SoftBank CEO Masayoshi Son told CNBC. . . .
>
> Son has long championed the benefits of artificial intelligence, investing billions of dollars in companies he believes can capitalize on it. Some of these companies include Uber Technologies and WeWork. He said all of the 70 or so investments of his Vision Fund have been focused on AI.
>
> "We are investing $100 billion in just one thing, AI," he said.

106. With that said, merging Sprint into T-Mobile was hardly a self-evident proposition to DT: by 2018, Sprint was America's number four wireless carrier (behind T-Mobile), laden with approximately $38 billion in debt.

107. If DT was to merge T-Mobile with Sprint, it needed a major value proposition for the combined entity.

108. Enter AI and DT's aggressive data-mining apparatus, which arrived at T-Mobile shortly after an agreement in principle was struck to bring Sprint's subscribers (and their data) into T-Mobile in early 2018.

## V. DT AND SOFTBANK AGREE TO COMBINE THEIR U.S. TELECOM HOLDINGS, AND DT PUSHES ITS AI STRATEGY ONTO T-MOBILE

109. As discussed in earlier in this Complaint, by early 2018, DT had worked for years to push for aggressive AI/ML-focused data policies at its subsidiaries and affiliates. However, that push had not yet come to T-Mobile US, a company over which DT did not have direct control, and a company locked in a fierce battle with Softbank-owned rival Sprint for number three—a distant number three, to Verizon and AT&T Wireless—in the United States wireless carrier market.

110. In April 2018, the two conglomerates struck a deal: they would combine their two U.S. telcos, T-Mobile and Sprint, and more importantly, their data. As Reuters reported:

> T-Mobile US Inc. and Sprint Corp. said on Sunday they had agreed to a $26 billion all-stock deal [to combine the two companies] and believed they could win over skeptical regulators because the merger would create thousands of jobs and help the United States beat China to creating the next generation mobile network.
>
> The agreement capped four years of on-and-off talks between the third and fourth largest U.S. wireless carriers, setting the stage for the creation of a company with 127 million customers that will be a more formidable

> competitor to the top two wireless players, Verizon Communications Inc. and AT&T Inc. . . .
>
> Verizon has 116 million U.S. wireless customers, according to a spokesman, while AT&T has 93 million branded customers, as of the first quarter.

111. The breakthrough in the merger occurred when DT and SoftBank agreed on a deal that would allow DT to retain majority board control over the combined venture and consolidate it on its books. Pursuant to the conglomerates' deal, DT would own 42 percent of the combined company, but would control its board, nominating 9 of 14 directors:

> The breakthrough in the companies' negotiations, first reported by Reuters on Thursday, came after T-Mobile majority-owner Deutsche Telekom AG and Japan's Softbank Group Corp., which controls Sprint, agreed on a structure that would allow Deutsche Telekom to continue to consolidate the combined company, which will have a market value of over $80 billion, on its books.
>
> Deutsche Telekom will own 42 percent of the combined company, and will control the board of the combined company, nominating nine of the 14 directors. [T-Mobile CEO John] Legere will also serve as a director.

112. DT's overwhelming board control over the combined T-Mobile entity would be accomplished by a voting rights agreement with Softbank that would give DT access to voting rights for 69 percent of T-Mobile shares:

> Tokyo-based SoftBank and Deutsche Telekom will sign a voting rights agreement that will give Deutsche Telekom access to voting rights for a total of 69 percent of T-Mobile shares.

113. With the promise of majority board control in a combined U.S. telecom leviathan, DT brought its groupwide strategy of aggressively centralized, widely accessible, AI data and models to T-Mobile. Indeed, within months of the DT-SoftBank agreement facilitating a T-Mobile/Sprint merger, T-Mobile at long last—and well behind its competitors, including Sprint—joined the AI arms race among US cellular providers. And it would adopt a reckless, ultimately very costly AI strategy straight from its controlling shareholder's playbook.

## VI. T-MOBILE BELATEDLY JOINS THE AI ARMS RACE

114. However, T-Mobile faced a problem to satisfy its newly-aggressive mandate from DT: Unlike its chief competitors Sprint, AT&T, and Verizon—and unlike DT's directly-controlled European NatCos and other subsidiaries—T-Mobile had not had a head start with AI-based applications as ML/AI came into its own in the mobile carrier industry.

115. Moreover, unlike its principal competitors (and even its corporate cousins in Europe) T-Mobile did not have armies of engineers and data scientists at its disposal when the imminent Sprint merger promised to bring the world's largest repository of mobile subscriber data—and corporate philosophy of not just DT, but Softbank—to T-Mobile's doors. Additionally, T-Mobile's computer systems were well behind its competitors' in sophistication and complexity.

116. In short, T-Mobile was starting the AI arms race in earnest well behind its principal competitors—and even its promised suitor, Sprint—in 2018. What T-Mobile did have, however, was a business model developed by its corporate (quasi-)parent DT for rapidly developing an AI training program across a large telecommunications organization.

117. And this business model—the same one developed by Susan Wegner and her T-Labs team over the past few years at DT—was deployed beat-for-beat in the United States at T-Mobile by its Board and management, as it raced to catch up to its competitors and its agreed suitor in a rapidly scaling AI/ML arms race.

118. Specifically, in order to rapidly develop AI/ML operations across its vast company, T-Mobile did not start a new division. It did not hire droves of engineers. Instead, it hired a small team of data scientists and engineers and gave them unfettered access to all of T-Mobile's data and systems—complete with a consolidated credential and data repository system that mirrored DT's "app store for data models," the one designed by DT's T-Labs division to allow DT's data scientists to "access data all over the company" for training purposes.

119. In contrast to the years of development by entire divisions at Sprint, AT&T, and Verizon, T-Mobile gave its crack team just four months to build out the entire infrastructure it needed to create and deploy AI and ML applications that could rival T-Mobile's competition. As a substitute for resources and time, T-Mobile (in

keeping with the DT T-Labs model) gave its new data scientists unlimited access to the entire company—including its live computer systems—with no meaningful supervision.

120. Indeed, because they were beholden to majority shareholder DT, the Individual Defendants and the Board aggressively implemented the DT mandate to massively centralize the sensitive data of millions of users. The Individual Defendants ensured, by design or because of motivated and reckless disregard for the risks, that T-Mobile failed to implement any means of limiting the risk of data centralization. As explained below, T-Mobile, under the management of the Individual Defendants, dismantled any safeguards around centralized data, including by providing a new crack team unfettered access to the company's data and resources. This dismantling made DT's grand AI vision and precut pattern easier to implement, but at the cost of externalizing the risk of data breaches onto shareholders and customers.

121. A November 2, 2018 blog post by T-Mobile engineers Jacqueline Nolis and Heather Nolis described the beginnings of T-Mobile's AI push:

> When executives at T-Mobile decided to see if artificial intelligence and machine learning could try to improve the customer experience at T-Mobile, our team was created. We were given four months and a small budget to prove the worth of AI and ML to the business by creating a valuable machine learning model and deploying it into live systems. We had the freedom to use whatever tools we wanted, as long as they could be maintained continuously.

122. While T-Mobile's competitors had long since seen the worth of AI, T-Mobile's new team would have to "prove th[at] worth" to decisionmakers at the company. And while AT&T, Sprint, and Verizon had already deployed AI in the field, T-Mobile had tasked its team with deploying a single model into its live systems. Notably, T-Mobile gave its newly-formed team discretion to use whatever tools they wanted. This was a feature, not a bug—designed by the Board, management, and Individual Defendants—to implement DT's AI and data arbitrage mandate.

123. With that discretion, T-Mobile's team, under the supervision of the Company's corporate officers and directors, including the Individual Defendants, predictably made unusual and objectively poor engineering decisions. For example, although most enterprises used sophisticated and robust programming languages, such as Python, to develop machine-learning applications, T-Mobile's team used the programming language R—a language used for statistical modeling and a favorite tool of Wegner's T-Labs group at DT.

124. While R could help T-Mobile's data scientists rapidly prove that their ML models had predictive capacity, the language was poorly suited to security, data management, and data infrastructure, as it lacked many of the software libraries available in other programming languages, like Python.

125. Nolis and Nolis recounted the reason for the unorthodoxy—rapid modeling and deployment:

> Despite being an incredibly popular language for exploratory analysis, data scientists are repeatedly told that R is not sufficient for machine learning—especially if those ML models are destined for production. Though much exploratory analysis and modeling is done in R, these models must be rebuilt in Python to meet DevOps and enterprise requirements. Our team doesn’t see the value in double work. We explore in R and immediately deploy in R. Our APIs are neural network models using R and TensorFlow in docker containers that are small and maintainable enough to make our DevOps team happy!

126. T-Mobile was not building robust applications using Python. It was building neural network models—mathematical systems designed to very loosely mimic how real neurons process information—without the enterprise-heavy guardrails widely implemented in other companies’ (and organizations’) deployments. The Individual Defendants, including management and the Board, all knew that a robust implementation would impede data sharing with DT, so they not only looked the other way, they encouraged rapid development without any of the industry-proven safeguards.

127. Moreover, as Nolis and Nolis explained, they were deploying the models in “docker containers”—self-contained systems that could be run on any server without configuration.

128. T-Mobile decided it would buck the trend of building robust applications—like DT's T-Labs group before it (but without any of the intrusive DT's board gave to Wegner and her colleagues in Europe), T-Mobile would train models first and ask questions later. Styled as cleverness in the November 2018 blog post, this would turn out to be hubris—and objectively dangerous to customer data—as shown again and again (and again) in the two-and-a-half years since. While it may have been hubris for engineers, it was precisely what T-Mobile's majority shareholder DT expected of the Board and management at T-Mobile, including Individual Defendants—rapid execution of DT's data and AI model-centralization plan at whatever cost to shareholders and customers.

## VII. T-MOBILE'S MODELS AND THE NEED FOR DATA CENTRALIZATION

129. In late 2018, T-Mobile decided to rapidly train models, not build out complex software and data infrastructure like its competitors. But in order to rapidly train models, T-Mobile needed to feed these models with vast quantities of data—and also constantly feed back results. To do this, T-Mobile streamlined access to data—and access to inferential data coming from its machine learning models—across the company. In fact, T-Mobile rapidly implemented a centralized credentialing and permission framework like that developed by Wegner's T-Labs team at DT.

130. The first project T-Mobile's data scientists undertook was a system that would use customer data to interact with a person calling T-Mobile. T-Mobile's engineers described the use cases in their November 2018 blog entry:

> Since starting down this machine-learning-in-production journey, we've found many valuable use cases. These include:
>
> - Determining if a person is a customer by the first question they message T-Mobile.
>
> - Predicting the intent of the conversation so the necessary data is ready for the T-Mobile care agent.
>
> - Looking for and presenting to the agent internal knowledge-base articles as the conversation progresses.

131. To streamline access to the data and inferential pipeline, T-Mobile's team created an Application Programming Interface ("API") to allow access to the model. As T-Mobile's engineers explained on its blog in 2018:

> The project team has done an incredible job in a six-month time frame. They've validated that AI/ML can enhance Customer interactions at T-Mobile, created an API to make their model accessible by our ecosystem, and created some pretty neat tech that can be shared with the community. With this new capability we not only have an additional tool to enhance our Customer interactions but also a blueprint on how to apply AI/ML to other products and services.

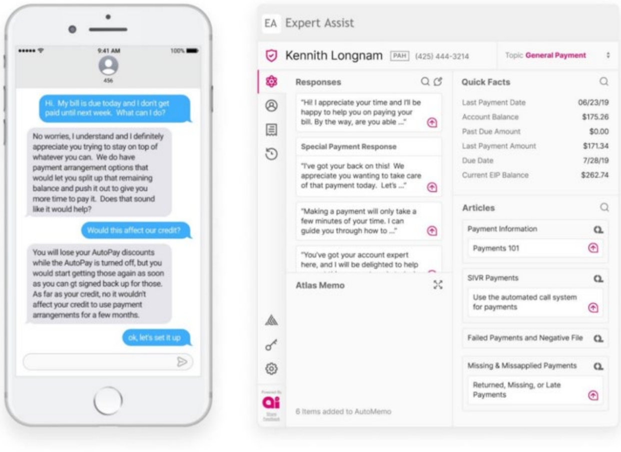
132. It was not only the output of the new machine-learning system that needed to be standardized and accessible across the organization. In fact, the data

underlying the AI model needed to be frequently retrained as new data came in. T-Mobile engineer Eric Hanson explained the problem in a May 13, 2020 blog post:

> Our business changes, our customers change, and our end users' needs change. The predictions of our production-deployed R services (and the functionality based on those predictions) have to change right along with them or the products we provide will quickly be discarded. This first became critical for us with a model we had to retrain at least daily. As we have described our patterns so far, the models themselves are built into the container (as ads files, h5 files, or other R-friendly mechanisms), requiring redeployment for a model change. This is somewhere between inefficient and untenable for a model that changes daily.

133. The crux of the problem was that the AI models would need to draw on all of the data—over and over again—and be updated every time new data was added into the mix. Each time retraining occurred, data would have to be loaded, a neural network trained, and then the trained network redeployed into live systems.

134. Put simply, for T-Mobile's models (like its customer service model, for example) to work properly, customer and prospective customer data had to be in one place—and accessed over and over again.



Hi. My bill is due today and I don't get paid until next week. What can I do?

No worries, I understand and I definitely appreciate you trying to stay on top of whatever you can. We do have payment arrangement options that would let you split up that remaining balance and push it out to give you more time to pay it. Does that sound like it would help?

Would this affect our credit?

You will lose your AutoPay discounts while the AutoPay is turned off, but you would start getting those again as soon as you can gt signed back up for those. As far as your credit, no it wouldn't affect your credit to use payment arrangements for a few months.

ok, let's set it up

"Hi! I appreciate your time and I'll be happy to help you on paying your bill. By the way, are you able ..."

Special Payment Response

"I've got your back on this! We appreciate you wanting to take care of that payment today. Let's ..."

"Making a payment will only take a few minutes of your time. I can guide you through how to ..."

"You've got your account expert here, and I will be delighted to help

6 Items added to AutoMemo

| | |
|---|---|
| Last Payment Date | 06/23/19 |
| Account Balance | $175.26 |
| Past Due Amount | $0.00 |
| Last Payment Amount | $171.34 |
| Due Date | 7/28/19 |
| Current EIP Balance | $262.74 |

Payment Information

Payments 101

SIVR Payments

Use the automated call system for payments

Failed Payments and Negative File

Missing & Missapplied Payments

Returned, Missing, or Late Payments

A customer care conversation and tool view with recommended articles on the lower right

135. T-Mobile described an example from its own systems: One of T-Mobile's new AI models used conversation text to predict internal wiki articles that a customer should be referred to. When new customer interactions were recorded or changes were made to the content of the underlying wiki pages, the model would have to be retrained to account for the changes. As T-Mobile's engineers explained on a company blog:

> As this is a wiki, both the content and usage change over time. Just as important—net-new content is introduced before applicable cases arise (for example content about new products, services, and offers). New content, changed content, and changes in usage patterns can each give rise to situations where today's useful content predictions will be irrelevant (or at least sub-optimal) tomorrow.
>
> If this were a simple database query, we'd change the data in the database and move on. It is not, however; it is a model trained on a combination of article text, customer conversations, and agent usage information. Some form of

> recurring retraining is required. In the case of the wiki model, we aligned to the potential publication of net-new information. That is generally a daily process so a daily retraining is where we started.

136. This repeat-data-access problem is even more acute when training and testing new models. Data scientists, writing programs in R, need to draw on the same data source to test new models. Then, when deployed, retraining requires repeated access to that same data, including any updates. In short, T-Mobile's bootstrapped machine learning infrastructure required massive, near-constant data access from a variety of sources—a problem Wegner had noted years earlier in her work for DT.

137. However, T-Mobile had built its systems on Docker containers and the R programming language. It did not have the sort of robust data-pipeline infrastructure used at companies like LinkedIn or Facebook. But instead of investing in building such infrastructure—or even a semblance of it—T-Mobile took a dangerous shortcut.

138. Specifically, T-Mobile centralized its data, centralized the credentials to access its databases, and created a single point from which its models could pull massive amounts of actual and potential customer data, including on test servers. This decision would end up with disastrous results for customers—and remains a danger to T-Mobile customers to this day.

139. It closely followed the pattern set out by DT for its NatCos. T-Mobile's DT-beholden Board and management, including the Individual Defendants, had

executed on DT’s mandate, by deliberate design, intentional disregard for risks, and extreme recklessness. T-Mobile’s management and board, including the Individual Defendants, never disclosed the massive risk T-Mobile was undertaking for majority shareholder DT, nor did they implement or enforce any safety constraints on the rapid implementation of DT’s AI and data mandate.

## VIII. T-MOBILE’S RECKLESS DATA AGGREGATION AND CENTRALIZATION

140. Modern machine learning and AI algorithms do not work like conventional computer programs. They learn directly from data. This means that their models, often mathematical or statistical in nature, must be “trained” across a representative set of data. And in order to train and test these data-hungry models, data must be aggregated, cleaned, and centralized. T-Mobile faced this data access hurdle when it set out to bootstrap a machine learning infrastructure in a matter of months in the face of years-long, well-resourced AI programs already launched by its principal competitors.

141. The company’s solution was reckless, objectively dangerous, and imperiled—and imperils—customer data. It also came straight from the playbook of T-Mobile’s largest shareholder: DT, whose T-Labs group had developed, promulgated, and worked to deploy across DT’s other NatCos and subsidiaries the precise sorts of risky AI training solutions T-Mobile ended up adopting in the United

States. T-Mobile's management and Board, including the Individual Defendants, implemented that playbook and looked the other way as to the massive risks.

142. In late 2018, T-Mobile was faced with the need to rapidly test and deploy machine learning and AI models, but did not implement the guardrails and infrastructure its competitors had already been working on for months, and in some cases, years. Chief among those guardrails was software infrastructure that would allow data segmentation and security.

143. T-Mobile's engineers, who had experience with model-building but not enterprise software development, used technology typically used by statisticians and academics, not seasoned computer programmers building complex systems.

144. Because their focus was on model training and testing rather than the safety of the data used for those models, T-Mobile's machine learning team cut corners—corners that needed to be cut to share data and AI models with controlling shareholder and parent, DT.

145. As DT's mandate required, the team's focus was on ease of testing and deployment—*i.e.*, the ability to test whether a model was effective, then quickly deploy that model—to the exclusion of robust (or even bare minimum) data security considerations.

146. For example, in order to speed along testing and deployment of machine learning models across its computer systems, T-Mobile developed a system

called qAPI. This allowed data across multiple databases to be queried through a common API. The qAPI architecture included a central repository with the keys to T-Mobile's entire data kingdom; even the credentials for separate databases across T-Mobile would be centrally stored in this system.

147. This massively centralized structure created a dangerous single point of failure for T-Mobile's information security. And it was the result of a deliberate tradeoff made by T-Mobile's developers—ignoring industry-standard, bare minimum information security practices (most glaringly, "don't store the access credentials for your entire ecosystem in a single repository accessible by test servers") so that T-Mobile's test servers could quickly and repeatedly query data from across the organization and use it to test and train the company's new machine-learning models.

148. The tradeoff was a reckless one—one that was not only unreasonable, but far from the industry practice. Indeed, respective machine learning applications should have had their own individualized access points to various subsets of data—and only to the data each application or model needed. T-Mobile made every piece of data stored in its databases centrally accessible—and then allowed test servers to freely and repeatedly access that central repository. None of this was even remotely normal, let alone acceptable. But T-Mobile did it—and, on information and belief, continues to do it—because it was executing a risky playbook already designed and

deployed by its largest shareholder, whose T-Labs subgroup pioneered a strategy of centralizing data, models, and credentials to boost DT's data-related profits.

### A. Machine Learning, AI, and the Need for Centralized Data

149. Unlike conventional computer programs, which are essentially a series of instructions programmed by developers and translated into machine-executable code, machine learning models are mathematical models designed to learn from data.

150. As one machine learning data scientist at IBM, Benjamin Manning, described on the site towardsdatascience.com, the learning process for a machine learning algorithm is not unlike how a child learns to ride a bike:

> One of my fondest childhood memories is of my father teaching me to ride my new bike. I think this was my first "real" hard knocks experience since my father didn't show me how to ride my bike, but rather allowed me to fail slightly each time I tried and eventually fell off. Seemingly, I'd never get there, but slowly and surely I deduced what I was doing wrong based on the lessons I learned about what I was doing right each time I tried to ride. Throughout my experiences and experiments, I adjusted each one of these variables until the outcome resembled some semblance of what was needed to breeze down our dead-end street on my own and ride with the fastest of my friends.
>
> Little did I know at the time, every iteration represented a learning experience regardless of the outcome—failure or success—I was learning how to manage things like balance, momentum, speed and even grit.

151. Although this class of algorithm, which has its roots in vector calculus, linear algebra, and statistics, is not new, it has only recently become viable as a method of decision-making at scale. This is largely due to the advent of powerful vector processors like GPUs and a series of breakthroughs in training artificial neural networks—mathematical models designed to learn in a manner akin to how a neuron in the brain learns—through repeated inputs and weighting.

152. It was only in the last several years that such neural networks could be deeply layered, massively increasing their capacity to learn from and detect complex patterns in data. As Wired Magazine explained in an August 2019 article, the basic concept (and indeed, much of the related technology) is quite old, but the breakthrough spurring the current revolution in machine learning came in 2012:

> Machine learning sounds modern, but it's one of the oldest ideas in computer science. In 1959, a room-filling computer called the Perceptron set a milestone in artificial intelligence when it learned to distinguish shapes such as triangles and squares.
>
> It was built on an approach to machine learning called artificial neural networks—which also power most of the AI projects grabbing headlines today. Neural networks in the cloud or even on our phones are behind virtual assistants and goofy photo filters.
>
> Neural networks old and new are based on math inspired by simple models of how neurons function in the brain. Alexa wasn't invented in 1959 because not long after the debut of the Perceptron, researchers mostly abandoned neural networks—it wasn't clear how they could be scaled

> up to tackle large problems. The technique spent decades as a fringe interest in computer science.
>
> Around 2012, the small community still working on the neural network approach to machine learning showed groundbreaking new results on speech and image recognition. Machine learning was suddenly the hottest thing in tech. This year, three researchers who brought about that revolution won the Turing Award, the Nobel Prize of computing.

153. Because these algorithms identify patterns in data—sometimes patterns imperceptible to humans—they are often designed to take as inputs many parameters, with some models having the capacity to look at millions of parameters (or many more).

154. A parameter can be a variable or a piece of information. For example, a basketball player's height, average points per game, and shoe size can all be parameters fed into machine learning models like deep neural networks.

155. It is often impossible to tell, however, which parameters together or alone will have the most predictive value for a given task. For example, it may well be that shoe size does not predict a basketball player's performance—yet when coupled with height and average points per game, the same piece of data might be quite useful.

156. An important part of training machine learning algorithms like neural networks is therefore the task of "feature selection." A data scientist's goal is often

to automatically select the variables that are going to have the most predictive value for a given task. As the Machine Learning Mastery Blog explains:

> Feature selection is also called variable selection or attribute selection.
>
> It is the automatic selection of attributes in your data (such as columns in tabular data) that are most relevant to the predictive model problem you are working.

157. The goal is often to minimize the number of features used, so that the simplest model for the task can be constructed:

> Feature selection methods can be used to identify and remove unneeded, irrelevant and redundant attributes from data that do not contribute to the accuracy of a predictive model or may in fact decrease the accuracy of the model.
>
> Fewer attributes is desirable because it reduces the complexity of the model, and a simpler model is simpler to understand and explain.

158. The process of homing in on the most important features often requires providing a superset of features and eliminating the features that do not improve a model's predictive accuracy.

159. That means that data, which includes many features, is split into distinct training and test sets (and in many cases an additional validation set). From there, the machine learning model is trained on the training set and its accuracy is measured against the test set.

160. This process is repeated until the predictive power of the model is maximized and the important features are identified.

161. After a feature is selected and a model is trained, the process is still not complete. Models need to be updated, which means that after they are deployed, they will have to be additionally trained (or perhaps retrained entirely) with a set of updated data.

162. For example, a user who lingers on a picture on Instagram provides data that Facebook then must use to update its model of that user's interests. If Facebook does not update its model with this new data, the user's feed of pictures become static and stale, reducing user engagement.

### B. T-Mobile's Data Centralization

163. The task ahead of T-Mobile was clear—and daunting—when the company began the hurried process of implementing DT's data, AI and model-sharing mandate. T-Mobile would have to rapidly train entirely new models to perform various tasks, such as predicting why a person is calling T-Mobile or whether a user is likely to purchase a particular additional product or service in a particular context.

164. Because T-Mobile's data scientists and engineers could not generally know *a priori* what pieces of data in the company's possession would be predictive

for each problem they set out to solve, they would often have to start with a broad universe of data.

165. From there, as a model was trained and refined, only a subset of that data would likely be necessary. However, the process of pulling the data for model training and testing is cumbersome and time consuming.

166. This is especially problematic when various forms of data are distributed across different databases, with different required credentials and perhaps different database schemas (relational structures).

167. Test systems need access to large universes of data—at least initially. Given T-Mobile's directive from DT to centralize data, coupled with its late start, T-Mobile's developers did not build a permissioned system that would carefully police which models, servers, and systems had access to what data. And, T-Mobile's DT-beholden management and Board, including the Individual Defendants, recklessly put no measures in place to ensure that any of the frantic bootstrapping would mitigate the risks of data breaches. Doing so would run afoul of the very object of DT's data arbitrage plans in the United States for T-Mobile.

168. Moreover, it was often impossible for T-Mobile's data scientists to tell whether a particular piece of customer data, no matter how apparently insignificant, would have a predictive effect—particularly in the aggregate, when combined with other data.

169. T-Mobile, with immense pressure from its DT-beholden management and Board, demanded that its new data scientists move fast. They needed to train, test, and deploy models to do in a matter of months what better-resourced competitors spent years fine-tuning. And to do that, T-Mobile's new models needed to repeatedly access and re-access massive amounts of consumer data from disparate sources. If T-Mobile did not devise a way to centralize that data, its development of new models could take years—as it had for T-Mobile's already-far-ahead competitors. More troubling, DT's plan required rapid centralization with unfettered access across its organization of subsidiaries and NatCos, and doing things the right way would frustrate that plan.

### C. T-Mobile Recklessly Cuts Corners with qAPI

170. Faced with the tradeoff of developing a robust data pipeline and infrastructure for its machine learning and testing on one hand, and the rapid deployment of trained models on the other, T-Mobile followed the DT T-Labs model—choosing expediency and ease of access organization-wide over all other considerations.

171. For example, to facilitate centralized data access across the company, T-Mobile developed technology called qAPI, which stands for query API. The goal of the software was to allow disparate systems and users—including test servers and

applications—to quickly access data from across T-Mobile in a centralized fashion using a standardized API.

172. T-Mobile described the system and its impetus in a November 7, 2019, blog post by Julio Zevallos:

> Designing and implementing test flows typically involves validating data with one or multiple databases. Whether it may be a simple test script, test frameworks such as Selenium (R), or test applications such as Tosca (R), querying the database directly is often not a good approach (from security and maintainability standpoints), and sometimes, not even fully supported.
>
> In order to remove the database connections from such tests, T-Mobile's Test Platform Engineering team developed qAPI (which stands for query API). qAPI eases the process by converting a database query to an API service that testers can integrate with in order to retrieve data in their test scripts. With this design, they can simply make an API call whenever needed, keeping their tests clean and modular. Additionally, if certain test frameworks don't provide the drivers needed to connect to certain databases, qAPI removes this constraint and allows more flexibility and expandability on database-type support.

173. The blog post was correct on one thing: it was not (and is not) best practice for apps to directly query databases. Unfortunately, qAPI did not resolve the attendant security problem with such querying—in fact, it exacerbated it. qAPI was not an intermediary designed to segment data. To the contrary, it was designed to ***unify*** data across multiple databases—and to do it seamlessly, even if a particular app was not configured to directly interact with a particular database. In short, qAPI

centralized and flattened otherwise segmented data, creating a single point of access to T-Mobile's entire data ecosystem. And it minimized access restrictions in doing so, including by facilitating and in fact prioritizing "sharing," including by "[m]aintaining queries on a user specified repository, where teams can save and update their queries on a key-value basis."

174. In other words, through qAPI an application, including a test application, could directly query several of T-Mobile's databases at once without having to be configured to query any particular database, and it could do so using information stored in centralized repositories. Once data was pulled from these databases, qAPI exerted no further control. The test app could do what it wanted with the data, including saving it locally in a flat file.

175. T-Mobile described the purported benefits of qAPI on its company blog. T-Mobile's purpose for qAPI was clear: to reduce the burden of pulling massive amounts of data across T-Mobile's various databases:

> Reduced effort: qAPI only needs database query and credentials to create an API by letting dynamic values be passed to queries through the body of a POST API call and automatically creating JSON response from database query output. Testers don't ***need to write a line of code to enable an API***.
>
> [. . .]
>
> Reusability and sharing: Maintaining all the queries on a user specified repository, where teams can save and update their queries on a key-value basis.

(emphasis added).

176. This sort of aggressive data (and indeed even model and credential) centralization and sharing across an entire far-flung organization was not only far from any enterprise best practice, it was nigh unheard of—except that it appeared to be a near beat-for-beat implementation of the groupwide "app store for data" strategy that had been developed and evangelized by Wegner and her T-Labs team for use at DT NatCos and subsidiaries.

177. T-Mobile's qAPI meant that any piece of software would have access to databases across the organization without having to implement any of the guardrails associated with database and data access. T-Mobile was clear that not a single line of bespoke code was needed to access disparate, initially siloed data.

178. Critically, qAPI allowed "credential" centralization. That meant that individual usernames and passwords or other database access keys would not have to be maintained by each app. They would be held by the API, which in turn would enforce access from querying apps. This meant that the credentials for every database would be centrally maintained—creating a single point of failure for T-Mobile's security.

179. Put simply, once compromised, qAPI offered the keys to T-Mobile's entire kingdom: access to any database connected to it, as credentials for each

database would not be required so long as an attacker had querying capability through the API.

180. As T-Mobile explained in its blog:

> Also, all database configurations are centralized in one location so if credentials ever need to be added or updated, they can be done in one location, rather than on a test by test basis.

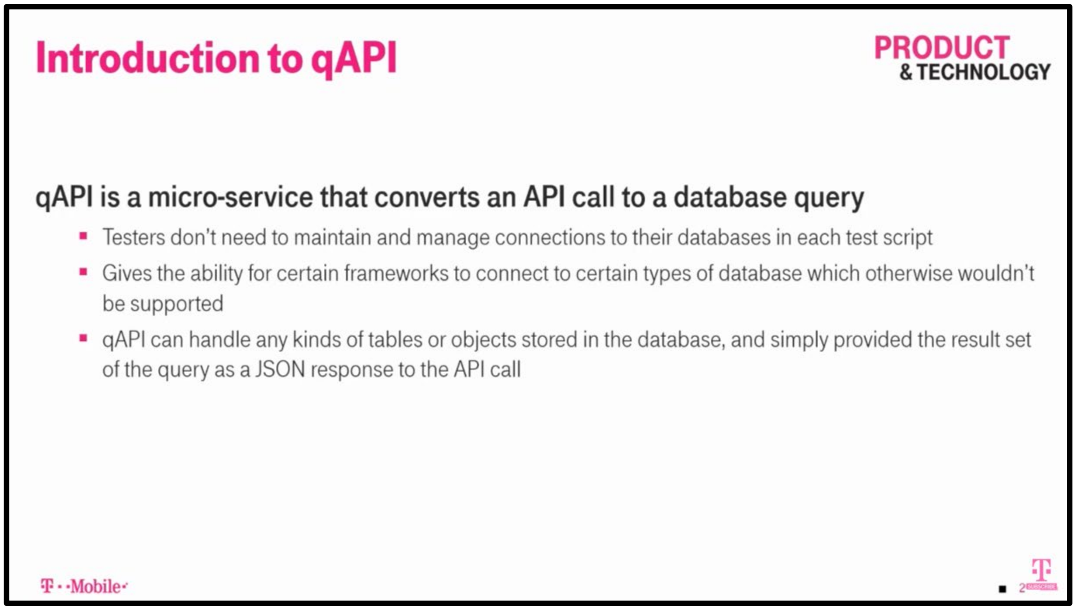
181. This was a reckless practice—and a deliberate part of the DT-beholden strategy set by T-Mobile's management and board, including the Individual Defendants.

182. As one security professional explained on a cybersecurity blog:

> [T]he practice of hardcoding credentials is increasingly discouraged as it poses formidable security risks that are routinely exploited by malware and hackers. In some cases, a threat actor (perhaps aligned with a nation-state) may insert hardcoded credentials to create a backdoor, allowing them persistent access to a device, application, or system.

183. qAPI not only centralized credentialing, it maintained all of T-Mobile's credentials as part of the system—a security practice outrageously far afield from the norm and the standard of care.

184. T-Mobile provided additional details about qAPI in a November 2019 video on its official YouTube channel.



## Introduction to qAPI

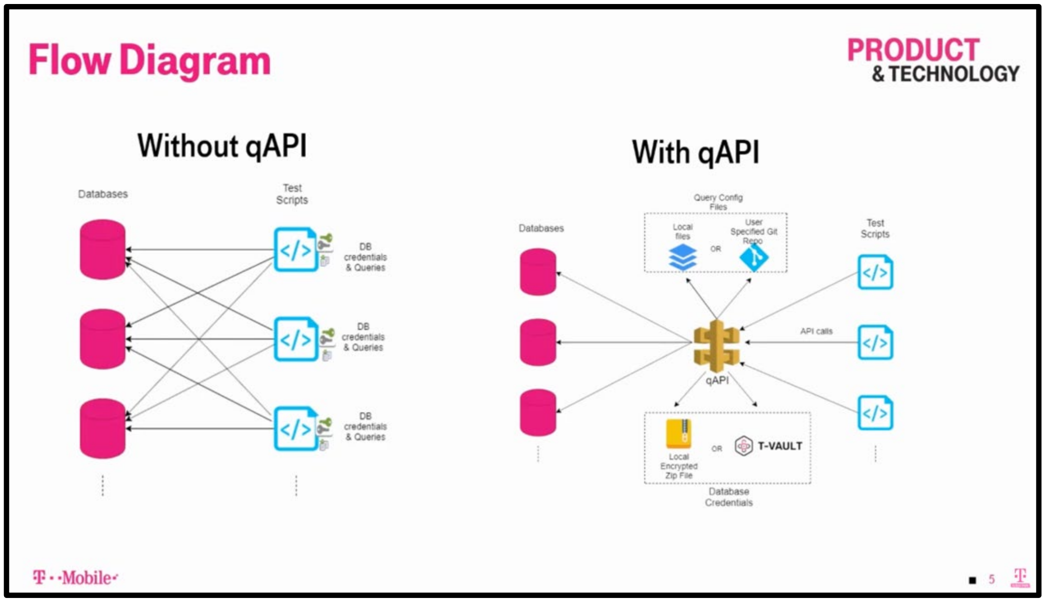
PRODUCT
& TECHNOLOGY

qAPI is a micro-service that converts an API call to a database query

- Testers don't need to maintain and manage connections to their databases in each test script
- Gives the ability for certain frameworks to connect to certain types of database which otherwise wouldn't be supported
- qAPI can handle any kinds of tables or objects stored in the database, and simply provided the result set of the query as a JSON response to the API call

185. As the video explained, the purpose was to allow test servers to access databases without having to maintain their own credentials: "[A]ll database configurations can be centralized in one location for all tests. This way, teams can configure these connections in one spot rather than on a test by test basis."

186. The video made the data credential centralization crystal clear with a diagram:



Flow Diagram

PRODUCT & TECHNOLOGY

187. As T-Mobile's diagram shows, the structure on the left (without qAPI) would require each test script to query each database separately. With qAPI (pictured on the right), however, access to all databases is centralized through qAPI.

188. This allows a test script to make queries from several databases at once without having to know the credentials and configurations of each database.

189. This structure essentially subverts any security restrictions on individual databases, making qAPI itself a centralized and single point of vulnerability.

### D. The Internal Threat and the Multiplying Vulnerability Created by Data Centralization

190. The problem with T-Mobile's data centralization is not simply that it creates a single point of attack for a malicious actor. The problem is also that it creates a single source from which a wide range of data stored across multiple

databases can be obtained—a poorly-protected single point of attack that also happens to store all the company's valuables without extra security. Unfortunately, the outrageous data centralization in T-Mobile's computer systems since the advent of the company's rush to catch up on machine learning is, for the company, a feature, not a bug.

191. Indeed, qAPI and other data centralization at T-Mobile was built in part to allow frictionless testing of systems and access from test servers. This meant that experimental software running on test servers—for example, new machine learning models being trained by T-Mobile's data scientists—could easily and repeatedly make queries that returned massive amounts of structured data.

192. If a test server itself was not secure or was somehow compromised, then all of the data, across any database that qAPI or other T-Mobile centralization software had access to, could be brought into that compromised system with no further control over the data. This was—and remains—endemic to the structure of T-Mobile's data centralization apparatus. And it closely models the data centralization systems designed by its largest shareholder—DT—for use at its various NatCos and subsidiaries.

193. Once data is queried using T-Mobile data centralization tools like qAPI, these tools do not control what happens to the data. A test system, for example, may copy data it obtained through qAPI or a similar tool. It can store that data locally. It

can transmit that data. There are no persistent controls on the data that is queried and saved by a test server (or any other system) through qAPI or another similar T-Mobile tool. As a result, a single compromised test server anywhere in the entire T-Mobile ecosystem can easily and durably access, save, and export the entirety of T-Mobile's data ecosystem—because T-Mobile ***designed its system that way***, including to facilitate its game of catch-up with AT&T, Sprint, and Verizon on machine learning.

194. As for qAPI, if a test system queries massive amounts of data from several databases and then locally saves that data, the data is as vulnerable to attack as the test server itself.

195. In other words, the single point of failure is multiplied. Data that is queried becomes accessible from any system that maintains or uses that data.

196. Unlike systems that are individually designed and configured to access only particular data sources and databases, the ability to access data from a centralized location means that every system that obtains that data must itself maintain robust security. That is, of course, not the sort of security deployed in test systems or in test programs—including at T-Mobile.

197. One example of a robust security architecture required to properly secure a system in which disparate data sources can be accessed from a centralized location would be an enterprise software infrastructure of the sort that T-Mobile's

machine learning and AI team affirmatively eschewed early on its design process, opting instead to use a notoriously insecure development stack designed for statistical analysis and academic research.

## IX. T-MOBILE EXPERIENCES REPEATED DATA BREACHES

198. Beginning in mid-2018, when T-Mobile began its rapid race to collect, mine, and monetize its customers' data, including through machine learning and AI, T-Mobile suffered repeated data breaches.

199. Each breach slowly revealed that a deeper problem existed at T-Mobile. This was not a case in which T-Mobile was simply—albeit serially—misconfiguring its software or its databases.

200. The data compromised by each breach made clear that T-Mobile never resolved the root problem. That is because the data centralization that made each breach possible was a feature, not a bug, to T-Mobile's developers and data scientists.

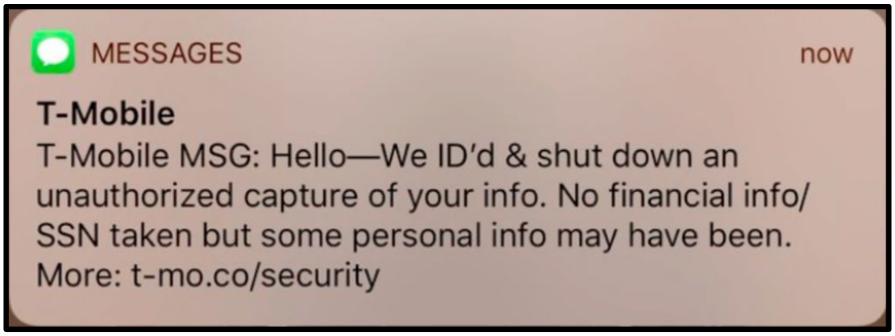
201. And this "feature" was a direct import from T-Mobile's largest shareholder: DT.

### A. The August 2018 Data Breach

202. On August 24, 2018, T-Mobile announced that it was hit by hackers who were able to gain access to personal information from roughly two million

customers, including the name, billing zip code, phone number, email address account number, and account type of users.

203. T-Mobile texted its users informing them that their personal information was taken:



T-Mobile

T-Mobile MSG: Hello—We ID'd & shut down an unauthorized capture of your info. No financial info/ SSN taken but some personal info may have been. More: t-mo.co/security

204. T-Mobile also posted the following announcement on its website:

> Dear Customer—
>
> Out of an abundance of caution, we wanted to let you know about an incident that we recently handled that may have impacted some of your personal information.
>
> Our cyber-security team discovered and shut down unauthorized access to certain information, including yours, and we promptly reported it to authorities, and no passwords were compromised. However, you should know that some of your personal information may have been exposed, which may have included one or more of the following: name, billing zip code, phone number, email address, account number, account type (prepaid or postpaid), and/or date of birth.

205. T-Mobile did not explain how the breach had occurred. More importantly, it did not explain how the hacker obtained access to customer data from a single attack.

206. T-Mobile, although claiming that “no passwords were compromised,” later admitted through a spokesman that encrypted passwords were in fact obtained.

207. Although encrypted, an attacker could easily crack passwords by brute force- or dictionary-attacking the encrypted passwords on a local machine.

208. The efficacy of such an attack depends significantly on the encryption used, but T-Mobile refused to tell customers any details. T-Mobile also doggedly stood by its misleading statement that no passwords had been compromised. As Motherboard recounted on August 24, 2018:

> When I asked why the company used that wording, the spokesperson said in a message: “Because they weren’t [compromised]. They were encrypted.”
>
> The spokesperson declined to specify how those passwords were encrypted, or what hashing algorithm was used. Hours after this story was published, security researcher Nicholas Ceraolo reached out claiming that the data exposed in the breach was more than what T-Mobile disclosed. The researcher shared a sample of allegedly compromised data that included a file called “use password” and what looks like a hash, which is a cryptographic representation of a password. (Ceraolo said he was not involved in the hack but obtained the sample from a “mutual friend.”)

209. To make matters worse, T-Mobile had used a weak hashing algorithm for its passwords, called MD5. As Motherboard further reported after the data breach:

> According to two different security researchers, with whom Motherboard shared that hash, it may be an encoded

> string hashed with the notoriously weak algorithm called MD5, which can potentially be cracked with brute-forcing attacks.

210. It was clear that T-Mobile customer passwords were vulnerable to a brute force attack, but T-Mobile did not take responsibility.

211. More importantly, T-Mobile never even addressed the truly important question—how did the attacker get access to so much data at once?

## B. The November 2019 Data Breach

212. On November 22, 2019, T-Mobile again suffered a data breach affecting approximately a million of its users. This time, the breach exposed customer names, billing addresses, phone numbers, account numbers, rate, plan, and calling features.

213. The exposed data constituted "customer proprietary network information" under telecom regulations, and T-Mobile was required to notify customers of the leak.

214. T-Mobile posted another disclosure on its website:

> Dear Customer,
>
> We want to let you know about an incident that we recently identified and quickly corrected that impacted some of your personal information.
>
> Our Cybersecurity team discovered and shut down malicious, unauthorized access to some information related to your T-Mobile prepaid wireless account. We promptly reported this to authorities. None of your

> financial data (including credit card information) or social security numbers was involved, and no passwords were compromised.
>
> The data accessed was information associated with your prepaid service account, including name and billing address (if you provided one when you established your account), phone number, account number, rate plan and features, such as whether you added an international calling feature. Rate plan and features of your voice calling service are "customer proprietary network information" ("CPNI") under FCC rules, which require we provide you notice of this incident.

215. The announcement included statements in response to various questions. Notably, when asked what T-Mobile planned to do to prevent future attacks, the company simply stated that data breaches were an inevitable part of their business:

> **What is T-Mobile doing to prevent this from happening again?**
>
> T-Mobile, like any other corporation, is unfortunately not immune to this type of criminal attack. Because of that, we are always working to improve security so we can stay ahead of malicious activity and protect our customers. We have a number of safeguards in place to protect your personal information from unauthorized access, use, or disclosure.

216. T-Mobile again refused to explain the elephant in the room—how a cyber-attacker able to obtain so much of its customer information at once.

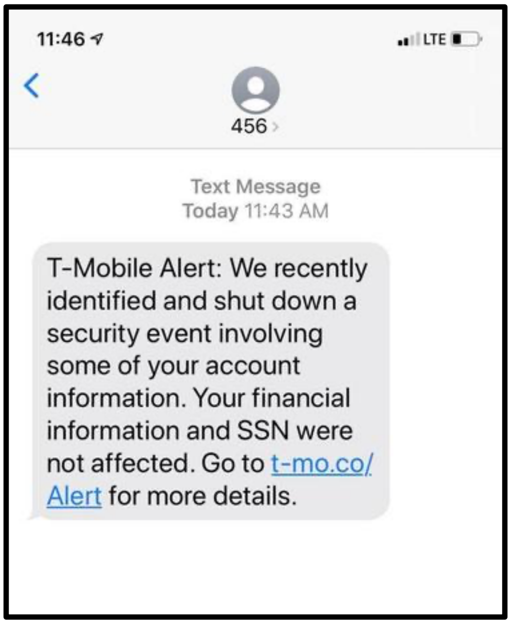
### C. The March 2020 Data Breach

217. On March 5, 2020, T-Mobile was hit with another data breach, exposing the same sort of customer information exposed in the previous breach, including names, addresses, phone numbers, account numbers, rate plans and features, and billing information.

218. This data breach, however, not only included customer data, but also T-Mobile employee data. T-Mobile admitted that the attacker gained access to "certain T-Mobile employee email accounts, some of which contained account information for T-Mobile customers and employees."

219. In addition, for some users, T-Mobile admitted, social security numbers, financial account information, and government identification numbers were exposed by the breach.

220. Again, T-Mobile notified users via text message:



Text Message
Today 11:43 AM

T-Mobile Alert: We recently identified and shut down a security event involving some of your account information. Your financial information and SSN were not affected. Go to t-mo.co/Alert for more details.

221. T-Mobile would not provide information as to how many people were impacted, but noted that both current and past customers were affected.

222. T-Mobile again said nothing as to how an attacker was able to obtain so much user information through a single attack. Nor did T-Mobile provide any information as to how it planned to prevent such attacks in the future.

223. T-Mobile's notice essentially repeated what it had told its customers after the last attack (the copy was still fresh—the last breach had happened just ten weeks before):

> **What Is T-Mobile Doing to Prevent This from Happening Again?**
>
> T-Mobile, like any other corporation, is unfortunately not immune to this type of criminal attack and we are always working to enhance security so we can stay ahead of this type of activity and protect our customers. We are also reviewing our security policies and procedures to enhance how we protect these systems.

224. This was a familiar refrain. And as it had done in the past, T-Mobile provided no information as to how it intended to prevent future attacks.

225. T-Mobile also offered affected customers "credit monitoring" services:

> **What Are We Doing?**
>
> For customers that received a link from us to this webpage, we are also offering free credit monitoring and identity theft detection services, provided by TransUnion.

226. The deeper problem—T-Labs-style data, model, and credential centralization and a reckless prioritization of access over security—was never fixed. T-Mobile's board, which was majority controlled by DT-affiliated directors, did nothing to change the way the company did business after its third major data breach in a year-and-a-half. T-Mobile's board, including Individual Defendants, had implemented no measures to supervise the massive centralization of data occurring at the company. It also failed to disclose that it had taken massive risks for majority-shareholder DT.

227. Unsurprisingly, the data breaches continued.

### D. The December 2020 Data Breach

228. In December 2020, T-Mobile experienced another data breach.

229. The December data breach compromised account information for 200,000 customers. The compromised information compromised included phone numbers, number of lines subscribed to, and in some cases, call-related information.

230. On December 30, 2020, T-Mobile issued a notice to customers that a data breach had occurred:

> Dear Customer,
>
> We are reaching out to let you know about a security incident we recently identified and quickly shut down that may have impacted some of your T-Mobile account information. The data access did not include names on the account, physical or email addresses, financial data, credit

> card information, social security numbers, tax ID, passwords, or PINs.
>
> **What Happened?**
>
> Our Cybersecurity team recently discovered and shut down malicious, unauthorized access to some information related to your T-Mobile account. We immediately started an investigation, with assistance from leading cybersecurity forensics experts, to determine what happened and what information was involved. We also immediately reported this matter to federal law enforcement and are now in the process of notifying impacted customers.
>
> **What Information Was Involved?**
>
> Customer proprietary network information (CPNI) as defined by the Federal Communications Commission (FCC) rules was accessed. The CPNI accessed may have included phone number, number of lines subscribed to on your account and, in some cases, call-related information collected as part of the normal operation of your wireless service.

231. Again, T-Mobile never explained how the information was compromised, nor did T-Mobile explain how it intended to prevent future data breaches. T-Mobile's board, including Individual Defendants, had implemented no measures to supervise the massive centralization of data occurring at the company. It also failed to disclose that it had taken massive risks for majority-shareholder DT.

## E. The February 2021 Data Breach

232. On February 9, 2021, T-Mobile disclosed yet another data breach to its customers. This time, T-Mobile sent a letter:

> Dear Customer:
>
> Recently, we detected unauthorized activity on your T-Mobile account, during which an unknown actor gained access to your account information, including personal information and your personal identification number (PIN). T-Mobile quickly identified and terminated the unauthorized activity however, we do recommend that you change your customer account PIN.

233. T-Mobile again treated the symptom, not the root problem (its data aggregation and centralization). That is, it offered two years of free credit monitoring:

> **What We Are Doing**
>
> We are offering you two years of free credit monitoring and identify theft detection services, provided by myTrueIdentity, from Transunion. Your activation code is _________. Please enroll by May 31, 2021 at www.mytrueidentity.com. Attached is a Step-by-Step Enrollment Guide as well as a How-to for signing up for Credit Monitoring Services.

234. T-Mobile also disclosed the information that was compromised:

> **What Information Was Involved?**
>
> The information accessed may have included your full name, address, email address, account number, social security number, customer account personal identification number (PIN), account security questions and answers, date of birth, plan information, and the number of lines subscribed to on your account.

235. The scope of the breach was yet another red flag that there was a deeper problem at T-Mobile. Once again—just like T-Mobile's August 2018, November

2019, March 2020, and December 2020 data breaches—the company's February 2021 breach allowed the attacker access to a concerningly broad set of data about customers.

236. Nonetheless, T-Mobile never explained the source of the compromised data; how it was kept; or what system the attacker had broken into that could have provided a single attacker with access to such a large amount of customer information in a single place.

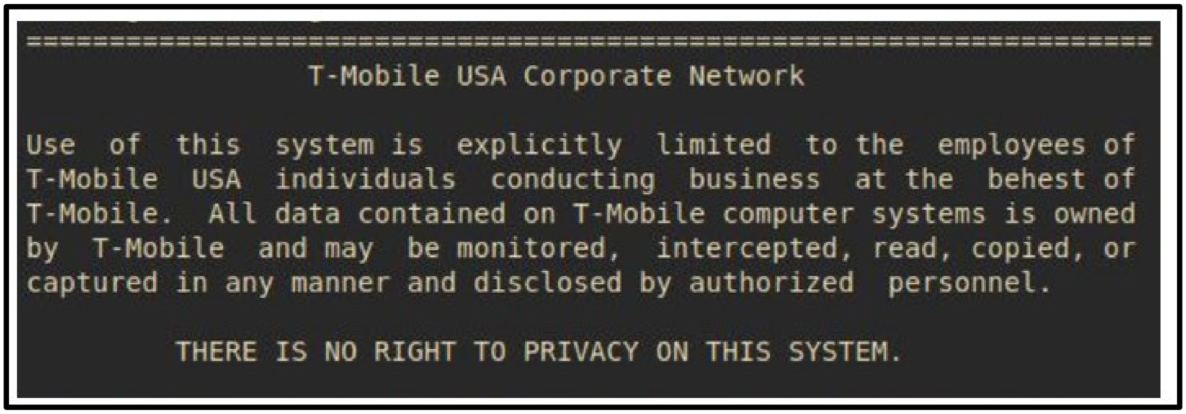
237. Moreover, once again, T-Mobile's officers and directors did nothing to fix the problem. T-Mobile's management and board, including Individual Defendants, had implemented no measures to supervise the massive centralization of data occurring at the company. They also failed to disclose that it had taken massive risks for majority-shareholder DT.

238. Then a few months later, the inevitable happened.

### F. The August 2021 Data Breach

239. In late July 2021, a twenty-one year-old hacker named John Binns discovered "an unprotected [T-Mobile] router exposed on the internet."[1] Binns "had been scanning T-Mobile's known internet addresses for weak spots using a simple tool available to the public," and eventually came across the following:

[1] Binns himself told his story to the Wall Street Journal in an article published August 27, 2021.



```
===================================================================
                T-Mobile USA Corporate Network

Use  of  this  system is  explicitly  limited  to the  employees of
T-Mobile  USA  individuals  conducting  business  at the  behest of
T-Mobile.  All data contained on T-Mobile computer systems is owned
by  T-Mobile  and may  be monitored,  intercepted, read, copied, or
captured in any manner and disclosed by authorized  personnel.

         THERE IS NO RIGHT TO PRIVACY ON THIS SYSTEM.
```

240. T-Mobile's "unprotected router exposed to the internet" was—like many other insecure servers, test systems, and other endpoints across T-Mobile's corporate network—plugged into T-Mobile's unprecedented data- and credential-centralization apparatus. Per the Wall Street Journal:

> Binns said he used that entry point to hack into the cellphone carrier's data center outside East Wenatchee, Wash., ***where stored credentials allowed him to access more than 100 servers.***
>
> "I was panicking because I had access to something big," he wrote. "Their security is awful."

(Emphasis added.)

241. In short, Binns found a single unsecured router publicly exposed on T-Mobile's network, and was quickly able to gain access to a centralized repository of credentials that allowed him the keys to T-Mobile's entire data kingdom, including ***more than 100 servers***. This matches the precise architecture of the qAPI system—and whether it was qAPI or some other similarly-reckless T-Mobile credential repository that allows a single insecure router to access, store, and ultimately

exfiltrate information from databases and systems across T-Mobile, it was the precise attack vector that T-Mobile affirmatively created (and maintained, through breach after breach after breach) with egregious data centralization as the company sought to rapidly train new machine learning models.

242. T-Mobile had, once again, been "pwned" by its own reckless design choices—and this time so egregiously that even the hacker himself was "panicking" at the degree of access he was allowed from a single point of failure. But for T-Mobile, this was simply the price of is largest shareholder DT's AI transformation strategy—and its business model of radically centralized data and access. T-Mobile hadn't stopped after data breach upon data breach since 2018, and it wasn't stopping now.

243. As Binns told the Wall Street Journal, "it took about a week to burrow into the servers that contained personal data about the carrier's tens of millions of current ***and former*** customers, adding that the hack lifted troves of data around Aug. 4" (emphasis added).

244. That is, T-Mobile's data and credential centralization not only allowed (and, by all indications, still allows) for unfettered access—from a single point of failure—to current customer information, but to information of millions of ***former*** (and indeed, prospective) customers as well. This is, as explained elsewhere in this Complaint, a T-Mobile feature, not a bug—because T-Mobile's machine learning

models must constantly train and retrain on massive, updated sets of consumer data to allow T-Mobile's data scientists to catch their employer up to its competitors when it comes to AI, and to serve the massive data needs of T-Mobile's principal shareholder DT.

245. On August 13, 2021, more than a week after Binn's Aug. 4 data exfiltration, a security research firm named Unit221B LLC reported to T-Mobile that an account was trying to sell customer data from the company. On August 15, 2021, T-Mobile publicly acknowledged it was investigating yet another data breach.

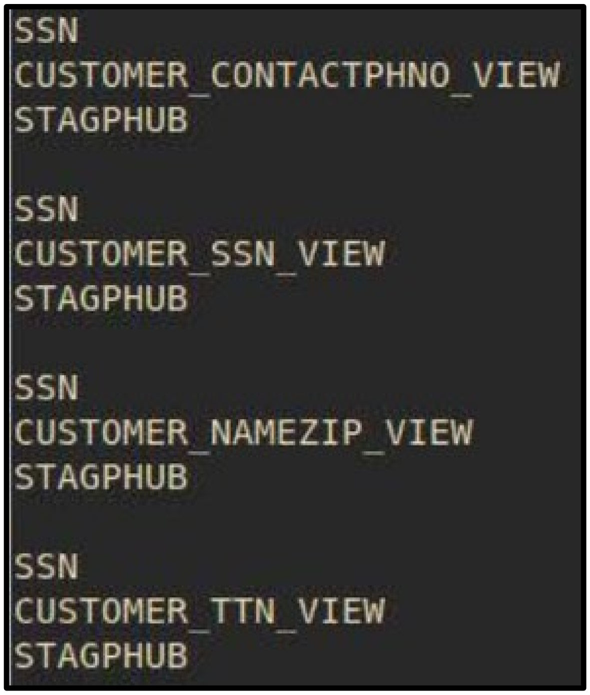
246. Eventually, T-Mobile confirmed that its systems had once again been breached, and that more than fifty million customer records stolen. In a statement, T-Mobile said "[w]e are confident that we have closed off the access and egress points the bad actor used in the attack"—essentially stating T-Mobile had secured the specific router that Binns had accessed by scanning T-Mobile IP addresses.

247. Yet T-Mobile did not commit to, or even acknowledge, the actual, systemic problem that had repeatedly imperiled customer information, and that continues to do so: T-Mobile's data centralization and systemwide access architecture, which it deploys through systems like qAPI to allow its data scientists to rapidly train machine learning models through repeat access to years of diverse data from throughout the company.

248. This ticking time bomb—which keeps going off every few months, most loudly in August 2021—is still armed and sitting inside T-Mobile's network. T-Mobile has done nothing to defuse it—and apparently will not do anything, absent intervention by this Court. Meanwhile, every current T-Mobile customer and tens of millions of former and prospective T-Mobile customers have their data imperiled every day by T-Mobile's reckless, inherently defective data architecture—and T-Mobile's board of directors, which is majority-controlled by DT, has not acted to solve or remedy this problem. Instead, it has simply authorized the payment of hundreds of millions of dollars of company money to settle off old liabilities from the August 2021 attack.

249. Shortly after the August 2021 breach, the Wall Street Journal explained: "Several cybersecurity experts said the public details of the hack and reports of previous T-Mobile breaches show the carrier's defenses need improvement. Many of the records reported stolen were from prospective clients or former customers long gone. 'That to me does not sound like good data management practices,' said Glenn Gerstell, a former general counsel for the National Security Agency."

250. A screenshot by Binns showed tables of personal information he was able to access on T-Mobile's servers, using a single compromised router:

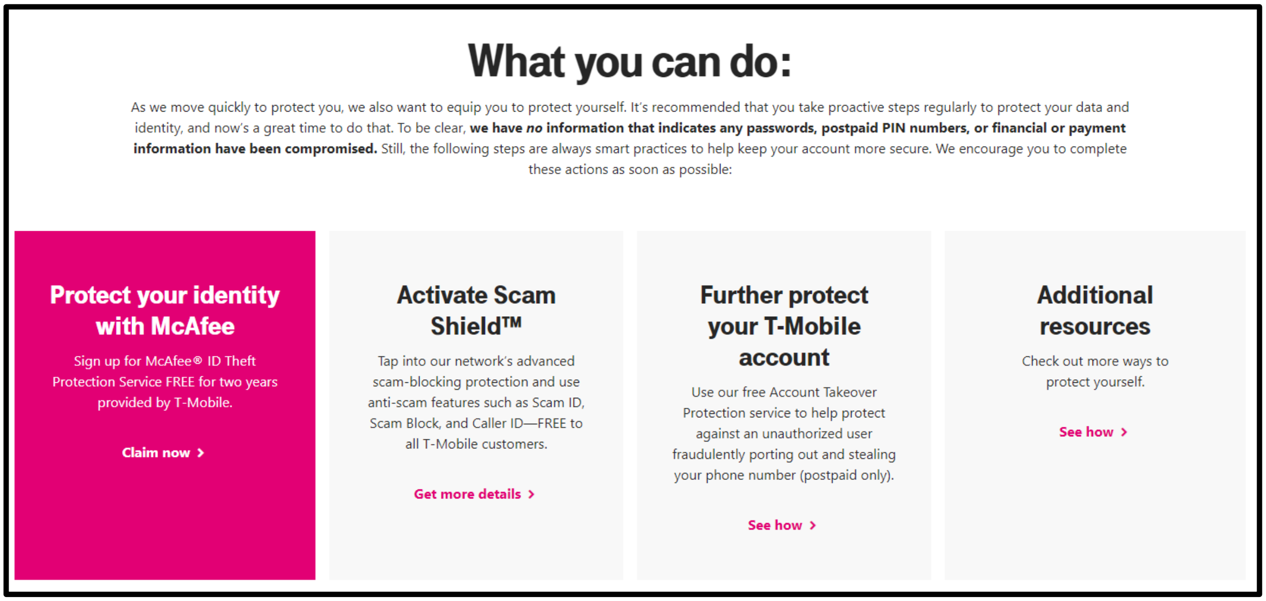


```
SSN
CUSTOMER_CONTACTPHNO_VIEW
STAGPHUB

SSN
CUSTOMER_SSN_VIEW
STAGPHUB

SSN
CUSTOMER_NAMEZIP_VIEW
STAGPHUB

SSN
CUSTOMER_TTN_VIEW
STAGPHUB
```

251. On August 19, 2021, T-Mobile set up a website providing "Notice of Data Breach" to its customers. T-Mobile stated that "[o]n August 17, 2021, T-Mobile learned that a bad actor illegally accessed personal data. Our investigation is ongoing, but we have verified that a subset of T-Mobile data had been accessed by unauthorized individuals and the data stolen from our systems did include some personal information."

252. According to T-Mobile, "[t]he exact personal information accessed varies by individual. We have determined that the types of impacted information include: names, drivers' licenses, government identification numbers, Social Security numbers, dates of birth, T-Mobile prepaid PINs (which have already been reset to protect you), addresses and phone number(s)."

253. T-Mobile offered—free of charge to customers (but costly to shareholders)—a host of identity-protection services to its customers to help mitigate the risks stemming from its latest data breach. The free services included two years of identity theft protection through McAfee, scam call protection (already available to T-Mobile customers), and an account takeover prevention service (available only to post-paid T-Mobile customers).



## What you can do:

As we move quickly to protect you, we also want to equip you to protect yourself. It's recommended that you take proactive steps regularly to protect your data and identity, and now's a great time to do that. To be clear, **we have *no* information that indicates any passwords, postpaid PIN numbers, or financial or payment information have been compromised.** Still, the following steps are always smart practices to help keep your account more secure. We encourage you to complete these actions as soon as possible:

### Protect your identity with McAfee

Sign up for McAfee® ID Theft Protection Service FREE for two years provided by T-Mobile.

**Claim now ›**

### Activate Scam Shield™

Tap into our network's advanced scam-blocking protection and use anti-scam features such as Scam ID, Scam Block, and Caller ID—FREE to all T-Mobile customers.

**Get more details ›**

### Further protect your T-Mobile account

Use our free Account Takeover Protection service to help protect against an unauthorized user fraudulently porting out and stealing your phone number (postpaid only).

**See how ›**

### Additional resources

Check out more ways to protect yourself.

**See how ›**

254. On August 20, 2021, T-Mobile provided the public and its customers with additional information about its latest data breach, including details on who was affected and what information was exposed. T-Mobile's forensic analysis determined that at least the following categories of information had been taken from its servers:

- 7.8 million current T-Mobile postpaid customer accounts that included first and last names, date of birth, SSN, and driver's license/ID information, phone numbers, and IMEI and IMSI information.
- 5.3 million current postpaid customer accounts that had one or more associated customer names, addresses, date of births, phone numbers, and IMEIs and IMSIs.
- Data files with information from about 40 million former or prospective T-Mobile customers, including first and last names, date of birth, SSN, and driver's license/ID information.
- 667,000 accounts of former T- Mobile customers that were accessed with customer names, phone numbers, addresses and dates of birth.
- An unspecified number of data files including phone numbers, IMEI, and IMSI numbers.
- Approximately 850,000 active T-Mobile prepaid customer names, phone numbers and account PINs. Similar information from additional inactive prepaid accounts was also accessed. Up to 52,000 names related to current Metro by T-Mobile accounts may have been included.

255. On August 27, T-Mobile CEO Mike Sievert posted an open letter on the T-Mobile website, which described the two-week period since the August 2021 data breach as "humbling for all of us at T-Mobile as we have worked tirelessly to

navigate a malicious cyberattack on our systems." According to Sievert, the data breach was now "contained and our investigation substantially complete."

256. Sievert wrote that "[o]n August 17th, we confirmed that T-Mobile's systems were subject to a criminal cyberattack that compromised data of millions of our customers, former customers, and prospective customers. Fortunately, the breach did not expose any customer financial information, credit card information, debit or other payment information but, like so many breaches before, some SSN, name, address, date of birth and driver's license/ID information was compromised."

257. Sievert stated that "[t]hrough our investigation into this incident, which has been supported by world-class security experts at Mandiant from the very beginning, we now know how this bad actor illegally gained entry to our servers and we have closed those access points. We are confident that there is no ongoing risk to customer data from this breach."

258. Sievert's letter continued:

> We recognize that many are asking exactly what happened. While we are actively coordinating with law enforcement on a criminal investigation, we are unable to disclose too many details. What we can share is that, in simplest terms, the bad actor leveraged their knowledge of technical systems, along with specialized tools and capabilities, ***to gain access to our testing environments*** and then used brute force attacks and other methods to make their way into other IT servers that included customer data. In short, this individual's intent was to break in and steal data, and they succeeded.

(Emphasis added.)

259. Sievert further wrote:

> Since confirming the breach, we have worked around the clock to understand impact and risk to customers and others and have done our very best to be transparent about those impacts as quickly as possible. This is not a one-and-done process. There is much work to do, and this will take time, and we remain committed to doing our best to ensure those who had information exposed feel informed, supported, and protected by T-Mobile.

260. In the same letter, Sievert stated that, as of August 27, 2021:

> [W]e have notified just about every current T-Mobile customer or primary account holder who had data such as name and current address, Social Security number, or government ID number compromised. T-Mobile customers or primary account holders who we do not believe had that data impacted will now see a banner on their MyT-Mobile.com account login page letting them know. We are also now working diligently to notify ***former and prospective customers***. Our goal is to ensure that we are providing clear information about how customers and those affected can protect themselves.

(Emphasis added.)

261. Finally, Sievert concluded:

> We know that the bad actors out there will continue to evolve their methods every single day and attacks across nearly every industry are on the rise. However, while cyberattacks are commonplace, that does not mean that we will accept them. T-Mobile is taking significant steps to enhance our approach to cybersecurity.
>
> Today I’m announcing that we have entered into long-term partnerships with the industry-leading cybersecurity

experts at Mandiant, and with consulting firm KPMG LLG. We know we need additional expertise to take our cybersecurity efforts to the next level—and we've brought in the help. These arrangements are part of a substantial multi-year investment to adopt best-in-class practices and transform our approach. This is all about assembling the firepower we need to improve our ability to fight back against criminals and building a future-forward strategy to protect T-Mobile and our customers.

As I previously mentioned, Mandiant has been part of our forensic investigation since the start of the incident, and we are now expanding our relationship to draw on the expertise they've gained from the front lines of large-scale data breaches and use their scalable security solutions to become more resilient to future cyber threats. They will support us as we develop an immediate and longer-term strategic plan to mitigate and stabilize cybersecurity risks across our enterprise.

Simultaneously, we are partnering with consulting firm KPMG, a recognized global leader in cybersecurity consulting. KPMG's cybersecurity team will bring its deep expertise and interdisciplinary approach to perform a thorough review of all T-Mobile security policies and performance measurement. They will focus on controls to identify gaps and areas of improvement. Mandiant and KPMG will work side-by-side with our teams to map out definitive actions that will be designed to protect our customers and others from malicious activity now and into the future. I am confident in these partnerships and optimistic about the opportunity they present to help us come out of this terrible event in a much stronger place with improved security measures.

As we learn and evolve, we will always work to keep you informed of any important updates or relevant changes. I also commit to you that while we're starting on this path with humility, we will bring to it the same Un-carrier energy that we have used for years to help transform the

> wireless industry for the benefit of consumers and businesses everywhere.

262. Once again—this time, 1000-odd words later—although T-Mobile admitted that it was indeed a badly-designed "testing environment[]" that gave Binns access to essentially the entirety of T-Mobile's customer (and indeed ***non***-customer) data, T-Mobile did not actually commit to fix what has led to six data breaches, of increasingly egregious scope, in the three years since the company began its ill-fated plunge into machine learning.

263. That is, T-Mobile did not promise to end, or even meaningfully address, its data and credential centralization practices—drawn from its largest shareholder DT—that permit single test servers to repeatedly vacuum data from databases across the company using stored credentials, combine all that data in a local copy, and store or exfiltrate it without meaningful controls.

264. T-Mobile did not promise to change its machine learning infrastructure; to end the use of qAPI and similar uniquely dangerous credential repositories that destroy multiple layers and types of data segregation and access control through their intentional design; to redesign its data access and analysis architecture to use industry-standard enterprise languages and designs; or promise any other concrete commitment that might actually protect the sensitive data of T-Mobile's current, former, and prospective customers within T-Mobile's centralized architecture.

265. The reason for this is clear: T-Mobile's flawed, dangerous data architecture was sourced from, and is deployed by T-Mobile's board and management, including the Individual Defendants, to the benefit of, the company's largest shareholder—DT. Meanwhile, the rest of the company—and its shareholders—incur hundreds of millions of dollars in concrete losses and unquantifiable future risk from these practices.

## X. T-MOBILE'S SYSTEMS REMAIN VULNERABLE

266. T-Mobile's systems remain vulnerable to attacks to this day.

267. Although T-Mobile claims to have sealed off the access point exploited in the company's most egregious recent data breach (the August 2021 breach), T-Mobile has not fixed the root problem—its centralization and aggregation of data. To the contrary, this dangerous practice, sourced directly from T-Mobile's largest shareholder DT, appears to continue to this day, likely for the benefit of DT's overall AI transformation initiative among its NatCos, subsidiaries, and affiliates.

268. Since August 2018—the very month that T-Mobile began centralizing data for machine learning purposes, and just weeks after DT's Susan Wegner explained the conglomerate's aggressive new model centralization and sharing initiatives would be rolling out "country by country" to DT's NatCos and subsidiaries—T-Mobile has suffered repeated, increasingly broad, data breaches. Indeed, there have been at list seven disclosed, major breaches of T-Mobile's

computer systems in the four years since the company began its frantic—and poorly planned—sprint toward AI.

269. The publicly-revealed contents of these data breaches, including the August 2021 breach, make clear that T-Mobile's ongoing data aggregation and centralization includes significant quantities of sensitive personal information—information that T-Mobile's data scientists and developers have made centrally available through T-Mobile's servers, such that individual points of failure across the company continue to expose mass quantities of personal information from disparate T-Mobile databases and systems.

270. There are many such individual points of failure in any corporate computer network. But T-Mobile's data architecture is not just any corporate computer network—it combines data centralization with credential centralization (through systems like qAPI), giving individual test servers unfettered access to sensitive databases throughout the entirety of T-Mobile upon the presentation of a single, intentionally-shareable, credential. And such a test server, which queries one or more databases, including through qAPI, can locally save a copy of the data it receives. That copy makes the test server itself an independently vulnerable point in T-Mobile's systems.

271. Likewise, if a software system has permission to make queries across databases, including through qAPI, then compromising that software system means compromising the databases to which the system has access.

272. Indeed, because credentials for multiple databases are centrally stored in T-Mobile's database intermediary systems, including qAPI, an attacker need not obtain any database credentials to compromise one or more databases with customer data. A single compromised test server can quickly—and because of the lack of controls on copying or exporting data, irreversibly—compromise sensitive information from databases across T-Mobile.

273. This is—based on the words of the attacker responsible for the August 2021 data breach—the precise attack vector used in at least one, and likely several, of the numerous breaches of T-Mobile systems since August 2018. And it is a vulnerability that has not been fixed, because it is endemic to T-Mobile's data centralization and machine learning enterprise, as currently designed and deployed.

274. T-Mobile's officers and directors, including the Individual Defendants, have known about the company's problematic, dangerous data centralization and sharing architecture, yet have declined to fix it. They have refused to do so despite breach after breach after breach—and now the payment of hundreds of millions of dollars in settlements and penalties from T-Mobile's coffers. That is because they are beholden to DT and act against the interest of other shareholders, including by

(a) implementing a dangerous data centralization strategy, (b) failing to disclose that their loyalty is divided and that they are implementing a strategy set or expected by majority shareholder DT, and (c) recklessly failing to put in place any safety or supervision measures to prevent further attacks.

275. The existence of database intermediaries like qAPI creates a massive security threat within T-Mobile's systems. This is because several databases and other stored data can be accessed with a single query. In other words, the querying software is able to obtain, consolidate, and structure data that would otherwise be stored separately in T-Mobile's systems.

276. For example, if T-Mobile stores encrypted customer passwords separately from account numbers, but nonetheless allows a software program querying databases through qAPI to combine that data, T-Mobile has coupled data that would otherwise be safely maintained in separate locations—requiring separate configurations and credentials to access.

277. Information from one database in an organization can frequently provide information to decrypt or otherwise reassemble disaggregated information from another database in that same organization, decreasing the effectiveness of safeguards like password hashing. This is one important security reason why organizations maintain separate databases in the first place, with distinct access controls, credentials, schema, and even technological pathways.

278. But T-Mobile's data architecture disassembles the access barriers and technological separation between distinct—often intentionally segregated—databases. Instead, because T-Mobile centrally maintains credentials and configurations for its databases, then allows software programs to query and combine their disparate data, T-Mobile essentially maintains a single consolidated pool of data. This single-point of access data centralization is incredibly dangerous—and a serious departure from well-accepted baseline data security and enterprise data storage practices. It does, however, meet with the overall profitability-based goals of DT's T-Labs division, as announced by Wegner and others.

279. T-Mobile's unusual—and dangerous—data centralization is the likely the reason why the seven known data breaches from August 2018 to December 2021 have repeatedly exposed wide, often facially disparate swaths of data, including sensitive data pertaining to current, former, and prospective customers.

280. Moreover, because T-Mobile uses data to train and deploy nascent machine learning and AI systems, the company keeps a diverse amount of data spanning a significant period of time—including decades of data that is unnecessary to the products and services sold by the company—in databases and systems that are centrally-accessible through aggregated credentials like qAPI, using software architecture built for mathematicians and scientists, not private enterprises combing

through sensitive information of millions of past, present, and potential future mobile subscribers.

281. If T-Mobile is not required to separate the data it maintains—and to do so effectively—it will continue to expose massive amounts of consolidated and structured data, including sensitive data of T-Mobile customers (and non-customers), through each and every software system and server that can access T-Mobile's data intermediaries such as qAPI. This will continue to cost the company and its shareholders hundreds of millions—and likely billions—of dollars. But the current slate of officers and directors—which is dominated by the interests of one large shareholder, DT—has not and will not do anything about this.

282. The consolidation of otherwise separated data significantly increases the odds of identity theft, fraud, and additional data breaches, all of which may result in significant costs to T-Mobile.

283. Moreover, the ability to query and structure data across T-Mobile's internal databases—a result of T-Mobile's extreme data and credential centralization—is exceptionally valuable to potential attackers, and will therefore likely repeatedly draw attacks designed to obtain such data. T-Mobile stands essentially alone among high-profile targets for the near-unlimited scope and unfettered access to data its centralized, single-point-of-failure system offers would-

be attackers. Yet the company's board and its executives have failed to act—except to pay out settlements and penalties.

284. Indeed, after each of six data breaches in three years, T-Mobile has failed to acknowledge any of these problems, instead repeating the refrain that data breaches are part and parcel of its business. Not so. T-Mobile exacerbates any baseline risks that exist by creating and centralizing a massive amount of consolidated and structured data for the taking—and maintaining a single point of vulnerability in its systems that is multiplied each time another system queries data from that vulnerable intermediary.

285. T-Mobile also provides credit monitoring, often through TransUnion. But that credit monitoring does not mitigate the ongoing risk posed by T-Mobile's data centralization and aggregation. Nor does the credit monitoring redress or remediate the credential-centralization practices that persist at T-Mobile to this day.

## XI. DT SOLIDIFIES ITS CONTROL OF T-MOBILE THROUGH BELOW-MARKET OPTIONS, AND ITS MERGER PARTNER SOFTBANK TRADES ITS STAKE IN T-MOBILE FOR A STAKE IN DT

286. While all this was going on at T-Mobile, DT was aggressively pushing to expand its stake and control in the company—and Softbank, meanwhile, was moving its stock holdings from the Sprint merger from T-Mobile to DT itself.

287. On April 1, 2021, DT's CEO Tim Höttges told DT shareholders that he expected the German conglomerate to secure direct ownership of T-Mobile in the medium term:

> Addressing the telecoms group's annual general meeting. Hoettges said he expected T-Mobile to return up to $60 billion to shareholders between 2023 and 2025.
>
> With its share of the proceeds, Deutsche Telekom would be able to raise its holding in T-Mobile to more than 50% from 43% at a price below current market levels secured with options, he said.
>
> "It's harvest time," said Hoettges.

288. But DT shareholders were anxious to see more profits for themselves from DT's stake in T-Mobile:

> Deutsche Telekom faced criticism from some shareholders . . . for proposing an unchanged dividend of 0.60 euros despite last year's strong results.
>
> In his speech, Hoettges said Deutsche Telekom would "further develop" its dividend in future years. . . .
>
> Group adjusted earnings . . . rose by 42% last year to $35 billion euros, driven by the $23 billion deal between T-Mobile and Sprint. As part of the takeover, Deutsche Telekom secured voting rights over the 9% stake in T-Mobile . . . still owned by former Sprint backer Softbank, enabling the German group to consolidate the results of its largest operating business.

289. In September 2021, DT agreed to raise its stake in T-Mobile by 5.3% to 48.4%, coming closer to direct control. DT did this through a $7 billion share-

swap deal with SoftBank. In this swap, DT agreed to receive millions of shares of T-Mobile stock from SoftBank (which shares had been acquired by Softbank through the Sprint merger), while SoftBank agreed to receive cash and a 4.5% stake in DT, establishing a direct shareholding relationship in DT. As Reuters reported:

> The latest transactions seek to lock down [the Sprint] deal by bringing Deutsche Telekom within touching distance of majority ownership over T-Mobile US—which accounts for three-fifths of group sales and is its most profitable unit.
>
> "This is a very attractive transaction for Deutsche Telekom and its shareholders to further benefit from the value creation potential in T-Mobile US and beyond," [Deutsche Telekom Chief Executive Officer Tim] Hoettges said.
>
> As part of the complex transaction, Deutsche Telekom will trigger option agreements, enabling it to lock in an average price of $109 per share for the 65 million T-Mobile shares it is acquiring, below last week's closing price of $136.
>
> Deutsche Telekom had options to lift its stake in T-Mobile US above 50%, Hoettges told a briefing, either by exercising further options or sitting out the $60 billion in share buybacks that the U.S. company plans in the coming years.

290. At the same time, DT wasn't the only AI-focused conglomerate seeking to monetize T-Mobile's data. SoftBank, whose founder Masayoshi Son had publicly proclaimed he was all-in on aggressive AI/ML plays in 2018 and 2019, divested itself of T-Mobile stock in favor of a giant stake in DT. As Reuters explained:

> For SoftBank founder Masayoshi Son, the share swap deal substitutes a residual stake in the U.S. business for a strategic holding in Deutsche Telekom, which is also present in a dozen European countries.
>
> "I'm a big believer that Deutsche Telekom stock has material upside," said SoftBank's chief operating officer, Marcel Claure, highlighting potential collaboration in areas such as digital payments, where Softbank has broad exposure.
>
> Softbank has agreed not to sell its Deutsche Telekom shares before the end of 2024.[[2]]

291. That same month, Fortune reported:

> Deutsche Telekom's management will support the appointment of SoftBank Chief Operating Officer Marcelo Claure to its supervisory board at the next general meeting. Claure also serves as a director at T-Mobile.

292. Meanwhile, as DT rushed to increase its still-minority, but controlling, stake in T-Mobile and SoftBank swapped its stake in T-Mobile with a multi-billion dollar, long-term stake in DT, the two conglomerates dominated—and continue to dominate—the US telecom's board of directors.

293. As of the date of this Complaint, seven members of T-Mobile's thirteen-member board—including Board Chairman Timotheus Höttges—are closely affiliated with DT.

[2] In April 2022, DT and SoftBank consummated the promised swap transaction.

294. Timotheus Höttges—the Chairman of T-Mobile's Board of Directors since 2013—is the CEO of DT.

295. Christian P. Illek—a T-Mobile director since November 2018—is DT's Chief Financial Officer.

296. Raphael Kübler—a T-Mobile director since April 2013—is a DT Senior Vice President.

297. Thorsten Langheim—a T-Mobile director since April 2013—is a DT executive, where he has held a succession of executive positions since 2009 and is a current member of DT's Board of Management.

298. Dominique Leroy—a T-Mobile director since November 2020—is a current member of DT's Board of Management.

299. Omar Tazi—a T-Mobile director since 2020—is currently a Senior Vice President at DT, where he focuses on technology and big data.

300. Marcelo Claure—a T-Mobile director since 2020—is the former COO of SoftBank and former CEO of SoftBank International. Claure is the signatory of a June 22, 2020 "Proxy, Lock-Up and ROFR Agreement" (the "Claure Proxy") between himself and DT that, among other things,

> irrevocably constitutes and appoints DT or any designee of DT, and any officer(s) or director(s) thereof designated as proxy or proxies by DT or its designee, as its attorney-in-fact and proxy in accordance with the Delaware General Corporate Law . . . to vote, or express consent or dissent with respect to

approximately 5 million shares of T-Mobile stock held in Claure's name (worth over $750 million as of T-Mobile's August 16, 2022, stock price). According to a June 2020 SEC disclosure, the Claure Proxy "prohibit[s]" Claure from "transfer of shares without the prior written consent of Deutsche Telekom until April 1, 2024, subject to certain exceptions." Additionally, as previously noted, in September 2021, DT agreed to support the appointment of Claure to DT's Board of Management at DT's next general meeting.

301. Additionally, during the time period of the events at issue in this complaint, several additional T-Mobile board members were closely affiliated with DT or SoftBank.

302. Michael Wilkens—a T-Mobile director between November 2020 and June 2022—was, during his entire tenure on the T-Mobile Board, a DT Senior Vice President. According to an April 2022 Form 8-K disclosure, "On April 20, 2022, Michael Wilkens notified T-Mobile . . . of his decision not to stand for re-election to [T-Mobile's] Board of Directors . . . in connection with his announced departure from Deutsche Telekom AG."

303. Srini Golapan—a T-Mobile director from 2019 to late 2020—is, and during his entire tenure on the T-Mobile Board was, a DT executive and a member of DT's Board of Management.

304. Lawrence H. Guffey—a T-Mobile director from 2013 to mid-2021—was a member of the Supervisory Board at DT prior to joining the T-Mobile board.

305. Ronald D. Fisher—a T-Mobile director from mid-to-late 2020—was a longtime SoftBank executive, including during his entire time on the T-Mobile board.

## XII. T-MOBILE'S AUGUST 2021 DATA BREACH COSTS SHAREHOLDERS $500 MILLION—AND THE PROBLEM IS STILL UNFIXED

306. On July 22, 2022, DT's reckless plan to aggressively mine T-Mobile for data cost the U.S. company's shareholders a massive, nine-figure sum. That day, T-Mobile agreed to pay a total of $500 million to settle multiple class-action suits stemming from the August 2021 data breach that exposed the data of tens of millions of people—and exposed T-Mobile's reckless data- and credential-centralization to the world.

307. However, despite promising to spend $500 million in shareholder money to settle old liabilities from T-Mobile's dangerous data- and credential-centralization practices, the proposed class settlement in the United States District Court for the Western District of Missouri did not actually fix the structural data security problem that led to a half-dozen major breaches in a three years at T-Mobile. That is, although the proposed settlement agreed to spend extra money on cybersecurity and to pay money to alleged victims, the proposed settlement did *not*

promise to end T-Mobile’s reckless, dangerous data- and credential-centralization practices, or to meaningfully restructure the company’s dangerous AI-driven data mining apparatus.

308. The reason for this is clear: T-Mobile is still being looted for data dollars by its European controlling shareholder, DT. This will continue for the foreseeable future, absent intervention by this Court.

## DERIVATIVE ALLEGATIONS

309. Plaintiff brings this action derivatively on behalf of T-Mobile, seeking redress for injuries suffered, and that will be suffered, by the Company directly and proximately caused by the Individual Defendants’ breaches of their fiduciary duties.

310. Plaintiff has owned T-Mobile stock continuously during the time of the wrongful course of conduct by the Individual Defendants alleged in this Complaint and continues to hold T-Mobile stock.

311. Plaintiff will adequately and fairly represent the interests of T-Mobile and its stockholders in enforcing and prosecuting its rights and has retained counsel competent and experienced in shareholder derivative litigation and other legally and technically complex litigation.

## DEMAND ON THE T-MOBILE BOARD IS EXCUSED AS FUTILE

312. Plaintiff has not made a demand on the T-Mobile Board to bring suit asserting the claims set forth in this Complaint because presuit demand is excused as a matter of law.

313. A majority of T-Mobile Board members suffer from conflicts of interest and divided loyalties that preclude them from exercising independent business judgment in considering both the events described in this Complaint and a pre-litigation demand pursuant to Rule 23.1.

314. In particular, six current members of T-Mobile's thirteen-member Board—Höttges, Illek, Kübler, Langheim, Leroy, and Tazi—are presently executives and/or Board of Management members at DT, the T-Mobile shareholder for whose benefit the breaches of fiduciary duty alleged in this Complaint were (and continue to be) performed:

- Director Höttges—the T-Mobile Board's Chairman—is currently CEO of DT.
- Director Illek is currently DT's Chief Financial Officer.
- Director Kübler is currently a DT Senior Vice President.
- Director Langheim is currently a DT executive and a member of DT's Board of Management.
- Director Leroy is a current member of DT's Board of Management.
- Director Tazi is currently a Senior Vice President at DT.

315. These six directors are plainly conflicted with respect to a litigation demand regarding the misconduct at issue in this Complaint, which originated from and was performed for the benefit of DT.

316. Additionally, a seventh member of T-Mobile's Board, Claure, is plainly conflicted with respect to a litigation demand regarding the misconduct at issue in this Complaint because of his close ties to DT and DT's significant, ongoing control over hundreds of millions of dollars of Claure's wealth. As noted earlier, Claure—the former COO of SoftBank and former CEO of SoftBank International—is the signatory of a June 22, 2020 "Proxy, Lock-Up and ROFR Agreement" (the "Claure Proxy") between himself and DT that, among other things,

> irrevocably constitutes and appoints DT or any designee of DT, and any officer(s) or director(s) thereof designated as proxy or proxies by DT or its designee, as its attorney-in-fact and proxy in accordance with the Delaware General Corporate Law . . . to vote, or express consent or dissent with respect to

approximately 5 million shares of T-Mobile stock held in Claure's name (worth over $750 million as of T-Mobile's August 16, 2022, stock price). Moreover, according to a June 2020 SEC disclosure, the Claure Proxy "prohibit[s]" Claure from "transfer of shares without the prior written consent of Deutsche Telekom until April 1, 2024, subject to certain exceptions." In September 2021, DT agreed to support the appointment of Claure—whose longtime company SoftBank recently swapped out some of its T-Mobile holdings for a substantial investment in *DT*—to *DT's* Board of Management.

317. Finally, an eighth member of T-Mobile's Board, Sievert, is conflicted and could not be expected to independently evaluate the allegations and claims at issue in this Complaint, because he was directly and personally involved as a T-Mobile officer—and indeed, the Company's President (2018-20) and CEO (2020-present) during the events at issue in this Complaint. In particular, Sievert was in charge of T-Mobile during the period in which its officers and directors turned the Company's data architecture into a dangerous, unregulated AI-training playground for the benefit of DT, leading to a series of high-profile data breaches and costing T-Mobile shareholders hundreds of millions of dollars (as set forth in this Complaint). Not only did Sievert personally oversee this scheme as the Company's President/COO and later CEO, Sievert reaped immense monetary sums from the Company over this same period. Since 2018, Sievert has received over $100 million in total compensation from T-Mobile in the form of salary, bonus, stock awards, non-equity plan compensation, and other compensation, making him one of the highest-paid telecommunications executives in the entire world. Indeed, Sievert would face substantial potential liability—including potential personal liability—based on the allegations and claims at issue in this Complaint, and could not be

expected independently evaluate them in a prelitigation demand for that reason alone.

318. In view of the above, at least eight current members of T-Mobile's thirteen-member board have such close ties—in most cases, direct financial and/or employment ties—to DT that they cannot independently evaluate matters concerning DT, such as a prelitigation demand regarding the facts and claims alleged in this Complaint.

319. As a result of the above, the T-Mobile Board cannot be expected to bring the claims asserted in this Complaint, and the actions of the Individual Defendants challenged in this Complaint are not protected from judicial scrutiny. Demand is therefore excused.

## **CLAIMS FOR RELIEF**

### COUNT I
### Breach of Fiduciary Duty
### (Against the Director Defendants)

320. Plaintiff repeats and realleges each and every allegation above as if set forth fully in this Count.

321. The Director Defendants, as directors of T-Mobile, are fiduciaries of T-Mobile and its stockholders. As such, they owe the Company the highest duties of good faith, fair dealing, due care, and loyalty.

322. The Director Defendants have breached their duty of loyalty by elevating and favoring the interests of DT over the interests of T-Mobile and its other stockholders, as set forth in this Complaint.

323. The Director Defendants owed (and owe) fiduciary duties to T-Mobile and its stockholders, including, without limitation:

- implementing, supervising, and overseeing the Company's data storage, data processing, and AI/machine learning systems and processes in a manner that accounted for due considerations of data privacy, cybersecurity, the Company's operational viability, and legal compliance;
- a fundamental duty to make good faith efforts to ensure that the Company's data centralization and AI systems were not a danger to T-Mobile customers and to the reputation of the Company; and
- a duty to ensure that the interests of a single shareholder—even a very large one—did not supplant the interests of the Company and its shareholders as a whole.

324. Instead, the Director Defendants have consciously breached their fiduciary duties and violated their corporate responsibilities by allowing reckless, overly aggressive data monetization and AI/machine learning efforts and processes driven by a single shareholder—DT—to supplant, overtake, and otherwise pervert

T-Mobile’s proper data privacy, cybersecurity, operational viability, and legal compliance concerns.

325. This resulted in a series of increasingly serious—and broad—data breaches over a short time period that the Director Defendants did nothing to stop, because they acted in the interest of DT rather than the Company as a whole. Instead, the Director Defendants paid hundreds of millions of dollars of shareholder money to settle liabilities due to their and officers’ wrongful actions at the behest and/or for the benefit of DT—yet the Director Defendants still have not dismantled or substantially redesigned the DT-sourced data- and credential-centralization program that has led to so many problems for the Company.

326. Additionally, in contemplating, planning, and/or effecting the conduct set forth in this Complaint, and consciously and deliberately serving the interests of DT to the detriment of T-Mobile and its other stockholders, the Director Defendants breached their duty of good faith toward, and acted in bad faith toward, T-Mobile.

327. The Director Defendants acted with divided loyalty (a) to implement DT’s data centralization strategy, and (b) to recklessly disregard the risks from that strategy. Director Defendants did not act with entire fairness or even reasonableness as to the strategy they implemented for controlling shareholder DT at the expense of other shareholders. Moreover, Director Defendants failed to disclose (a) their

divided loyalties, and (b) the risks to the company of their AI and data centralization strategy and/or failure to supervise such a strategy.

328. As a direct and proximate result of the Director Defendants' conscious failure to perform their fiduciary duties, T-Mobile has sustained significant damages both financially and to its corporate image and goodwill. Such damages to T-Mobile caused by Director Defendant's misconduct include substantial penalties, fines, damage awards, settlements, and expenses. Moreover, absent injunctive relief, these damages and other injuries to the Company will continue.

329. Plaintiff has no adequate remedy at law.

## COUNT II
## Breach of Fiduciary Duty
## (Against the Former Director Defendants)

330. Plaintiff repeats and realleges each and every allegation above as if set forth fully in this Count.

331. The Former Director Defendants, as directors of T-Mobile, were fiduciaries of T-Mobile and its stockholders. As such, they owed the Company the highest duties of good faith, fair dealing, due care, and loyalty.

332. The Former Director Defendants breached their duty of loyalty by elevating and favoring the interests of DT over the interests of T-Mobile and its other stockholders, as set forth in this Complaint.

333. The Former Director Defendants owed fiduciary duties to T-Mobile and its stockholders, including, without limitation:

- implementing and overseeing the Company's data storage, data processing, and AI/machine learning systems and processes in a manner that accounted for due considerations of data privacy, cybersecurity, the Company's operational viability, and legal compliance;
- a fundamental duty to make good faith efforts to ensure that the Company's data centralization and AI systems were not a danger to T-Mobile customers and to the reputation of the Company; and
- a duty to ensure that the interests of a single shareholder—even a very large one—did not supplant the interests of the Company and its shareholders as a whole.

334. Instead, the Former Director Defendants consciously breached their fiduciary duties and violated their corporate responsibilities by allowing reckless, overly aggressive data monetization and AI/machine learning efforts and processes driven by a single shareholder—DT—to supplant, overtake, and otherwise pervert T-Mobile's proper data privacy, cybersecurity, operational viability, and legal compliance concerns. This resulted in a series of increasingly serious—and broad—data breaches over a short time period that the Former Director Defendants did

nothing to stop, because they acted in the interest of DT rather than the Company as a whole.

335. Additionally, in contemplating, planning, and/or effecting the conduct set forth in this Complaint, and consciously and deliberately serving the interests of DT to the detriment of T-Mobile and its other stockholders, the Former Director Defendants breached their duty of good faith toward, and acted in bad faith toward, T-Mobile.

336. The Former Director Defendants acted with divided loyalty (a) to implement DT's data centralization strategy, and (b) to recklessly disregard the risks from that strategy. Former Director Defendants did not act with entire fairness or even reasonableness as to the strategy they implemented for controlling-shareholder DT at the expense of other shareholders. Moreover, Former Director Defendants failed to disclose (a) their divided loyalties, and (b) the risks to the company of their AI and data centralization strategy and/or from their failure to supervise such a strategy.

337. As a direct and proximate result of the Former Director Defendants' conscious failure to perform their fiduciary duties, T-Mobile has sustained significant damages both financially and to its corporate image and goodwill. Such damages to T-Mobile caused by Director Defendant's misconduct include substantial penalties, fines, damage awards, settlements, and expenses.

338. Plaintiff has no adequate remedy at law.

### COUNT III
### Breach of Fiduciary Duty
### (Against Sievert, As An Executive Officer of T-Mobile)

339. Plaintiff repeats and realleges each and every allegation above as if set forth fully in this Count.

340. Defendant Sievert, as an executive officer of T-Mobile, is a fiduciary of the Company and its stockholders. As such, he owed (and owes) the highest duties of good faith, fair dealing, due care, and loyalty.

341. Sievert has breached his duty of loyalty by elevating and favoring the interests of DT over the interests of T-Mobile and its other stockholders, as set forth in this Complaint. The conduct of Sievert as officer of T-Mobile is not shielded by 8 Del. C. § 102(b)(7).

342. Sievert, as an executive officer of T-Mobile, owed fiduciary duties to T-Mobile and its stockholders, including, without limitation:

- implementing and overseeing the Company's data storage, data processing, and AI/machine learning systems and processes in a manner that accounted for due considerations of data privacy, cybersecurity, the Company's operational viability, and legal compliance;

- had a fundamental duty to make good faith efforts to ensure that the Company's data centralization and AI systems were not a danger to T-Mobile customers and to the reputation of the Company; and
- had a duty to ensure that the interests of a single shareholder—even a very large one—did not supplant the interests of the Company and its shareholders as a whole.

343. Instead, Sievert, as an executive officer of T-Mobile, consciously breached his fiduciary duties and violated his corporate responsibilities by allowing reckless, overly aggressive data monetization and AI/machine learning efforts and processes driven by a single shareholder—DT—to supplant, overtake, and otherwise pervert T-Mobile's proper data privacy, cybersecurity, operational viability, and legal compliance concerns. This resulted in a series of increasingly serious—and broad—data breaches over a short time period that Sievert, as an executive officer of T-Mobile, did nothing to stop, because he acted in the interest of DT rather than the Company as a whole. Instead, while Sievert was CEO, T-Mobile paid hundreds of millions of dollars of shareholder money to settle liabilities due to Sievert's and others' wrongful actions at the behest and/or for the benefit of DT—yet Sievert and T-Mobile's other officers still have not dismantled or substantially redesigned the DT-sourced data- and credential-centralization program that has led to so many problems for the Company.

344. Additionally, in contemplating, planning, and/or effecting the conduct set forth in this Complaint, and consciously and deliberately serving the interests of DT to the detriment of T-Mobile and its other stockholders, Sievert, as an executive officer of T-Mobile, breached his duty of good faith toward, and acted in bad faith toward, T-Mobile.

345. Sievert acted with divided loyalty (a) to implement DT's data centralization strategy, and (b) to recklessly disregard the risks from that strategy. Sievert did not act with entire fairness or even reasonableness as to the strategy he implemented on behalf of controlling shareholder DT at the expense of other shareholders. Moreover, Sievert failed to disclose (a) his divided loyalties, and (b) the risks to the company of the AI and data centralization strategy and/or his failure to supervise such a strategy.

346. As a direct and proximate result of Sievert's conscious failure to perform his fiduciary duties as an executive officer of T-Mobile, T-Mobile has sustained significant damages both financially and to its corporate image and goodwill. Such damages to T-Mobile caused by Sievert's misconduct as an executive officer include substantial penalties, fines, damage awards, settlements, and expenses. Moreover, absent injunctive relief, these damages and other injuries to the Company will continue.

347. Plaintiff has no adequate remedy at law.

## PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

(a) for an order declaring that the Individual Defendants breached their fiduciary duties to the Company;

(b) for other appropriate injunctive relief;

(c) for an order awarding damages, together with pre- and post-judgment interest to the Company;

(d) for an order requiring the immediate disgorgement of all profits, benefits, and other compensation obtained by Sievert as a result of his breaches of fiduciary duties;

(e) for an order requiring the immediate disgorgement of all fees and other compensation earned by the Individual Defendants as a result of their service on T-Mobile's Board or any Board Committee;

(f) for Plaintiff's costs and expenses incurred in this action, including, but not limited to, experts' and attorneys' fees; and

(g) for such other and further relief as may be just and proper.

OF COUNSEL:

BATHAEE DUNNE LLP

Brian J. Dunne (to be admitted pro hac vice)
Edward M. Grauman (to be admitted pro hac vice)
901 South MoPac Expressway
Barton Oaks Plaza I, Suite 300
Austin, TX 78746
Tel.: (213) 462-2772

Yavar Bathaee (to be admitted pro hac vice)
Andrew C. Wolinsky (to be admitted pro hac vice)
445 Park Avenue, 9th Floor
New York, NY 10022
Tel.: (332) 322-8835

*Attorneys for Plaintiff*

*/s/ Joseph L. Christensen*
Joseph L. Christensen (#5146)
McCollom D'Emilio Smith Uebler LLC
2751 Centerville Road, Suite 401
Wilmington, DE 19808
(302) 468-5960

*Attorneys for Plaintiff*

DATED: September 16, 2022