ALMEIDA LAW GROUP LLC
Victor J. Sandoval (SBN 344461)
111 W. Ocean Blvd Suite 426
Long Beach, California 90802
(562) 534-5907
victor@almeidalawgroup.com

David S. Almeida (*pro hac vice* forthcoming)
849 W. Webster Avenue
Chicago, Illinois 60614
(312) 576-3024
david@almeidalawgroup.com

Counsel for Plaintiff & the Proposed Class

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

SPENCER CHRISTY, *individually and on behalf of all others similarly situated*,

Plaintiff,

vs.

LENOVO (UNITED STATES) INC.,

Defendant.

Case No.

CLASS ACTION COMPLAINT

1. VIOLATION OF THE ELECTRONIC COMMUNICATION PRIVACY ACT, 18 U.S.C. § 2510, *et seq.*
2. VIOLATIONS OF CALIFORNIA INVASION OF PRIVACY ACT, CAL. PENAL CODE § 631
3. VIOLATION OF CALIFORNIA INVASION OF PRIVACY ACT, CAL. PENAL CODE § 632
4. UNJUST ENRICHMENT
5. INVASION OF PRIVACY
6. INTRUSION UPON SECLUSION
7. COMPREHENSIVE COMPUTER DATA AND ACCESS AND FRAUD ACT, CAL. PENAL CODE § 502, *et seq.*
8. VIOLATION OF CALIFORNIA'S UNFAIR COMPETITION LAW, CAL. BUS. & PROF. CODE § 17200, *et seq.*

DEMAND FOR JURY TRIAL

Plaintiff Spencer Christy ("Plaintiff"), individually and on behalf of all others similarly situated, brings this class action lawsuit against Lenovo (United States) Inc. ("Lenovo" or "Defendant") and alleges, upon personal knowledge as to his own actions and his counsel's investigation and upon information and good faith belief as to all other matters, as follows:

INTRODUCTION

1. This case raises critically important issues at the intersection of privacy, commercial surveillance, and national security.

2. In April 2025, the U.S. Department of Justice implemented the Data Security Program, a national security program codified at 28 C.F.R. Part 202, known as "Bulk Data Transfer Rule," and more formally known as the "Rule Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons" (the "Bulk Sensitive Data Transfer Rule" or the "DOJ Rule").

3. The impetus for the DOJ Rule was that the U.S. government determined that the export of Americans' behavioral data to hostile foreign regimes or entities under their jurisdiction constitutes an "unusual and extraordinary threat . . . to the national security and foreign policy of the United States that has been repeatedly recognized across political parties and by all three branches of government."[1]

4. The DOJ Rule was thus implemented to prevent adversarial countries from acquiring large quantities of behavioral data which could be used to surveil, analyze, or exploit American citizens' behavior.

5. To prevent any potential for mass surveillance, the DOJ Rule prohibits transferring Americans' bulk sensitive personal data to entities tied to "countries of concern."

6. Currently, the "countries of concern" are China, Cuba, Iran, North Korea, Russia, and Venezuela. The Rule also limits access by "covered persons," meaning (i) individuals who

[1] Justice Department Implements Critical National Security Program to Protect Americans' Sensitive Data from Foreign Adversaries, U.S. DOJ (Apr. 11, 2025), *available at* https://www.justice.gov/opa/pr/justice-department-implements-critical-national-security-programprotect-americans-sensitive (last visited January 29, 2026; internal quotation omitted).

either reside in "countries of concern" or are controlled by entities in those countries or (ii) entities that are organized or chartered under the laws of, or have their principal place of business in, a country of concern, or are owned 50% or more by such entities.

7. Such bulk sensitive data includes the personal identifiers and associated communications at issue in this case.

8. The DOJ Rule makes clear that sending American consumers' information to Chinese entities through automated advertising systems and associated databases with the requisite controls is prohibited. The examples provided by DOJ in the DOJ Rule correlate with the types of data flows at issue in this case.[2]

9. Lenovo, and its foreign parents, have repeatedly faced scrutiny from federal regulators and members of Congress over concerns that their data practices facilitate surveillance by the Chinese government. Regulators and members of Congress have warned that Lenovo functions as a conduit for state directed data collection targeting American residents.

10. In direct violation of the DOJ Rule, Lenovo—through its automated advertising infrastructure and associated databases—transmits Plaintiff's and potentially millions of other American consumers' data to China.

11. This putative class action lawsuit results from that unlawful data-sharing of American citizens' sensitive information with a foreign adversary of the United States in direct violation of the DOJ Rule.

12. As detailed herein, Lenovo knowingly and systematically used communications and associated covered personal identifiers intercepted from American citizens for the purpose of sharing U.S. consumers' data with covered persons without the safeguards required by U.S. law.

13. When Plaintiff visited www.lenovo.com (the "Website") to browse for products and, ultimately, to purchase a Legion Tower 7i Gen 10 (Intel) with RTX™ 5080, Defendant facilitated the interception and disclosure of the full-page context—including full-string URLs revealing the pages viewed and product view—and persistent identifiers—including IP addresses, advertising IDs, and cookie data—to third parties.

[2] *See, e.g.,* 28 C.F.R. §§ 202.214(b)(7); 202.228(c)(2).

14. Lenovo then used the intercepted communications and identifiers for its own purposes including transmitting the intercepted communications and identifiers to covered persons—which includes entities, like the Lenovo Group, organized or chartered under the laws of, or having their principal place of business in, a country of concern, like China—in violation of the DOJ Rule.

15. This transmission enabled Lenovo, and its foreign parents, to link Plaintiff's browsing activity to his identity, track his behavior, and build detailed profiles reflecting his interests, location, habits and other private attributes.

16. In the hands of a foreign adversary, such data can be used to assemble detailed behavioral profiles, identify psychological or financial weaknesses, and monitor individuals in sensitive roles including, but not limited to, jurists, military personnel, journalists, politicians, or dissidents.

17. The disclosure of such data to anyone is a profound invasion of privacy but when that data is disclosed to foreign adversaries, it is also a direct threat to national security as it greatly increases the potential for coercion, reputational harm, and/or blackmail.

18. The conduct alleged herein gives rise to numerous individual and representative claims under federal and state law including, but not limited to, the Electronic Communications Privacy Act, 18 U.S.C. § 2510, *et seq.* ("ECPA"), because Lenovo used consumers' intercepted communications with the intention and for the purpose of disclosing that data in furtherance of a criminal or tortious act; specifically, the unlawful transfer of consumers' bulk sensitive personal data to a prohibited foreign entity in violation of the DOJ Rule.

PARTIES

19. Plaintiff Spencer Christy is and was at all relevant times, an individual and resident of the City of San Francisco in San Francisco County, California. Plaintiff intends to remain in California indefinitely and makes his permanent home there.

20. Lenovo is a corporation organized under the laws of Delaware with its principal place of business located at 1009 Think Place in Morrisville, North Carolina 27560.

//

JURISDICTION AND VENUE

21. This Court has subject matter jurisdiction over this putative class action lawsuit pursuant to 28 U.S.C. § 1331 because Plaintiff asserts an individual and representative claim under the ECPA, a federal statute.

22. The exercise of federal subject matter jurisdiction is also appropriate pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) ("CAFA"), because (i) at least one member of the Class is a citizen of a different state than any Defendant, (ii) there are more than 100 members of the Class, (iii) the aggregate amount in controversy exceeds $5,000,000, exclusive of interests and costs, and (iv) none of the exceptions apply to this action.

23. This Court has personal jurisdiction over Lenovo because it conducts business in this judicial district and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in the judicial district.

24. Venue is proper pursuant to 28 U.S.C. § 1391(b) because Plaintiff resides in this judicial district and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred here.

DIVISIONAL ASSIGNMENT

25. Pursuant to Local Rules 3.2(c) and 3.5(b), assignment to the San Francisco Division is proper because a substantial part of the events giving rise to Plaintiff's claims occurred in San Francisco County, and Plaintiff resides in San Francisco County.

FACTUAL ALLEGATIONS

A. LENOVO AND THE LENOVO GROUP

26. Lenovo makes, markets, and sells computers, computer accessories, and related products like tablets, monitors, servers, and storage.

27. Lenovo is a U.S.-based operating subsidiary of Lenovo Group Limited ("Lenovo Group"), a Hong Kong-incorporated multinational technology company with its principal corporate operations headquartered in Beijing, China.

28. The Lenovo Group maintains a significant presence in China and is subject to Chinese law, including China's National Intelligence Law, Cybersecurity Law, and Data Security

Law.

29. These laws require Chinese companies and individuals to secretly cooperate with government surveillance efforts and to grant authorities unrestricted access to private user data.

30. The Lenovo Group's operations are subject to Chinese government control, oversight, and compelled disclosure obligations.

31. The Lenovo Group's largest shareholder is Legend Holdings Corporation ("Legend"), a Chinese investment holding company based in Beijing.[3]

32. Legend was established by the Chinese Academy of Sciences ("CAS"), which is a state institution operating under the authority of the People's Republic of China.

33. Legend's predecessor received initial capital and institutional sponsorship from CAS and its affiliated commercialization vehicles.[4]

34. CAS, through its wholly owned investment arm, Chinese Academy of Sciences Holdings Co., Ltd., and related state-controlled entities, retains significant ownership, governance rights, and strategic influence over Legend.[5]

35. Through Legend's position as Lenovo Group's largest shareholder, these structural ties create enduring institutional and financial connections between Lenovo Group and the Chinese state.

B. THE BULK SENSITIVE DATA TRANSFER RULE

36. The DOJ Rule restricts or prohibits U.S. persons from engaging in covered data transactions with covered persons.

37. A U.S. person includes, *inter alia*, "any entity organized solely under the laws of

[3] Shareholding Structure | Lenovo, *available at* https://investor.lenovo.com/en/ir/shareholding.php (last visited January 28, 2026).

[4] Legend Holdings Company History, *available at* https://www.legendholdings.com.cn/History_en/index.aspx?nodeid=1044 (last visited January 28, 2026).

[5] Articles of Association of Legend Holdings Corporation, June 2025, *available at* https://ir.legendholdings.com.cn/media/1246/articles-of-association-2025.pdf (last visited January 28, 2026).

the United States or any jurisdiction within the United States (including foreign branches)[.]" 28 C.F.R. § 202.256.

38. A "covered person" includes, *inter alia*, "a foreign person … that is organized or chartered under the laws of, or has its principal place of business in, a country of concern[.]" *Id*. § 202.211.

39. A "country of concern" includes, *inter alia*, "China," which means "the People's Republic of China, including the Special Administrative Region of Hong Kong and the Special Administrative Region of Macau, as well as any political subdivision, agency, or instrumentality thereof." *Id.* §§ 202.208, 202.601

40. A "covered data transaction" is "any transaction that involves any access by a country of concern or covered person to any government-related data or bulk U.S. sensitive personal data and that involves: (1) Data brokerage; (2) A vendor agreement; (3) An employment agreement; or (4) An investment agreement." *Id.* § 202.210.

41. "Bulk U.S. sensitive personal data" means "a collection or set of sensitive personal data relating to U.S. persons, in any format, regardless of whether the data is anonymized, pseudonymized, de-identified, or encrypted, where such data meets or exceeds the applicable threshold set forth in § 202.205." *Id.* § 202.206

42. Section 202.205 sets forth the applicable thresholds for being considered "bulk" data. "Bulk" means "any amount of sensitive personal data that meets or exceeds the [listed] thresholds at any point in the preceding 12 months, whether through a single covered data transaction or aggregated across covered data transactions involving the same U.S. person and the same foreign person or covered person[.]" *Id.* § 202.205.

43. The applicable threshold for "covered personal identifiers" is that "collected about or maintained on more than 100,000 U.S. persons[.]" *Id*.

44. The term "covered personal identifiers" means "any listed identifier: (1) In combination with any other listed identifier; or (2) In combination with other data that is disclosed by a transacting party pursuant to the transaction such that the listed identifier is linked or linkable to other listed identifiers or to other sensitive personal data." *Id.* § 202.212.

45. The term "listed identifier" means "any piece of data in any of the following data fields: (a) Full or truncated government identification or account number (such as a Social Security number, driver's license or State identification number, passport number, or Alien Registration Number); (b) Full financial account numbers or personal identification numbers associated with a financial institution or financial-services company; (c) Device-based or hardware-based identifier (such as International Mobile Equipment Identity ('IMEI'), Media Access Control ('MAC') address, or Subscriber Identity Module ('SIM') card number); (d) Demographic or contact data (such as first and last name, birth date, birthplace, ZIP code, residential street or postal address, phone number, email address, or similar public account identifiers); (e) Advertising identifier (such as Google Advertising ID, Apple ID for Advertisers, or other mobile advertising ID ('MAID')); (f) Account-authentication data (such as account username, account password, or an answer to security questions); (g) Network-based identifier (such as Internet Protocol ('IP') address or cookie data); or (h) Call-detail data (such as Customer Proprietary Network Information ('CPNI'))." *Id.* § 202.234.

46. The effective date of the DOJ Rule was April 8, 2025. *Id.* § 202.216

47. Under the DOJ Rule, "no U.S. person, on or after the effective date, may knowingly engage in a covered data transaction involving data brokerage with a country of concern or covered person." *Id.* § 202.301 (a "Prohibited Data Transaction").

48. A "data brokerage" means "the sale of data, licensing of access to data, or similar commercial transactions, excluding an employment agreement, investment agreement, or a vendor agreement, involving the transfer of data from any person (the provider) to any other person (the recipient), where the recipient did not collect or process the data directly from the individuals linked or linkable to the collected or processed data." *Id.* § 202.214

49. Similarly under the DOJ Rule, "no U.S. person, on or after the effective date, may knowingly engage in a covered data transaction involving a vendor agreement, employment agreement, or investment agreement with a country of concern or covered person unless the U.S. person complies with the security requirements (as defined by § 202.248) required by this subpart D and all other applicable requirements under this part." *Id.* § 202.401 (a "Restricted Data

Transaction").

50. An "investment agreement" means "an agreement or arrangement in which any person, in exchange for payment or other consideration, obtains direct or indirect ownership interests in or rights in relation to: (1) Real estate located in the United States or (2) A U.S. legal entity." *Id.* § 202.228.

51. The "security requirements" defined by section 202.248 means "the Cybersecurity and Infrastructure Agency ('CISA') Security Requirements for Restricted Transactions E.O. 14117 Implementation, January 2025." *Id.* § 202.248.

52. The CISA Security Requirements for Restricted Transactions E.O. 14117 Implementation, January 2025, require certain organizational- and system-level requirements—including, *inter alia*, implementing certain organizational cybersecurity policies, practices, and requirements; implementing logical and physical access controls to prevent covered persons or countries of concern from gaining access to covered data that that does not comply with the data-level requirements; implementing risk assessment and mitigation strategies outlining how implementation will prevent access to covered data that is linkable, identifiable, unencrypted, or decryptable using commonly available technology by covered persons and/or countries of concern—and certain data-level requirements—including, *inter alia*, applying data minimization and data masking strategies to reduce the need to collect, or sufficiently obfuscate, respectively, covered data to prevent visibility into covered data, and applying encryption techniques to protect covered data during the course of restricted transactions.[6]

53. As detailed above, Lenovo is a U.S. person and the Lenovo Group is a covered person.

54. As detailed above and below, Lenovo engages in Prohibited or Restricted Data Transactions with the Lenovo Group, without the requisite security requirements, in violation of the DOJ Rule.

[6] *See, e.g.,* Security Requirements For Restricted Transactions Pursuant To Exec. Order 14117, Preventing Access To Americans' Bulk Sensitive Personal Data And United States Government-Related Data By Countries Of Concern *available at* https://www.cisa.gov/sites/default/files/2025-01/Security_Requirements_for_Restricted_Transaction-EO_14117_Implementation508.pdf

C. LENOVO'S WEBSITE USES TRACKERS WHICH EXPOSE AMERICAN'S BEHAVIORAL DATA TO FOREIGN ADVERSARIES.

55. When a user lands on the homepage of Website, the Website loads numerous first- and third-party tracking implementations that measure and record user data.

56. These tracking technologies including, but not limited to, web beacons, pixels, software development kits, APIs, JavaScript, real-time bidding and other scripts, and cookies, are small pieces of code that Lenovo intentionally integrated into the Website to track user behavior and to transmit data to first- and third-party platforms.

57. Lenovo intentionally programmed and deployed on the Website such tracking technologies, provided by TikTok, Facebook, Microsoft, Google, Adobe, Index Exchange, Inc., Wunderkind, Snap, Inc., and Liveramp, among numerous others (collectively and/or individually, the "Tracking Technologies").[7]

58. Through the Tracking Technologies, Lenovo collects bulk personal data, from users of the Website. This data includes persistent identifiers—including IP addresses, advertising IDs, and cookie data—and the full-page context—including full-string URLs revealing the pages viewed and product viewed.

59. On information and good faith belief, Lenovo has collected or maintained this sensitive personal data relating to more than 100,000 U.S. persons (including Plaintiff and the putative class members) following the effective date of the DOJ Rule, and therefore this

[7] While Plaintiff's investigation is necessarily ongoing, he has, to date, identified 55 scripts on the Website, belonging to Index Exchange, Inc., Smaato Inc., Facebook, Inc., Ströer Group, Roku, Inc., Criteo SA, FreeWheel, Improve Digital BV, ID5 Technology Ltd, Tapad, Inc., Bounce Exchange, Alphabet, Inc., PubMatic, Inc., Weborama, eyeota Limited, Adform A/S, Virtual Minds AG, TripleLift, Snap Inc., Adobe Inc., Amazon Technologies, Inc., Lotame Solutions, Inc., Sharethrough, Inc., Teads (Luxenbourg) SA, AudienceProject, Quantcast Corporation, OpenX Technologies Inc, The Trade Desk Inc, mediarithmics SAS, Magnite, Inc., Smartadserver S.A.S, The Nielsen Company, LiveRamp Holdings, Inc., Neustar, Inc., Bombora Inc., IPONWEB GmbH, Semasio GmbH, Amobee, Inc, Reddit Inc., and Flashtalking Inc. *available at* https://themarkup.org/blacklight?url=https%3A%2F%2Fwww.lenovo.com%2F&device=mobile&location=us-ca&force=false (last visited January 27, 2026). On information and good faith belief, this list is only a portion of the Tracking Technologies that Defendant implemented on the Website.

information constitutes "bulk U.S. sensitive data" under the DOJ Rule.

60. Indeed, publicly available web traffic reports estimate that 13.35 million U.S.-based devices visited the Website in December of 2025, alone.[8]

61. Without appropriate safeguards or excluding covered foreign parents, Lenovo knowingly permits access to, or transfer of, such bulk U.S. sensitive personal data to entities or persons that qualify as covered persons under the DOJ Rule, including its foreign parents that are directly or indirectly controlled by persons in China, such as the Lenovo Group.

62. Lenovo's actions create undue risks to national security and to the privacy of U.S. persons because providing access to sensitive personal data to covered persons is prohibited or restricted without strict compliance with the statutes and regulations promulgated under Executive Order 14117 and related federal law.

63. Despite the sensitivity of this data, Lenovo does not require users to validly consent to the operation of the Tracking Technologies.

64. As a result, Website users' personal information, including persistent identifiers (*e.g.,* cookie IDs, device IDs, mobile advertising IDs, and IP addresses), device metadata (*e.g.*, screen resolution, browser version, operating system, and language settings), and contextual information such as full URLs and referring pages are surreptitiously obtained by the Tracking Technologies.

65. Such user data can be correlated and combined with other data sets to compile comprehensive user profiles that reflect consumers' behavior, preferences, and demographics.

66. Those in possession of this information can gain deep understanding of users' behavioral traits and characteristics.

67. By installing and using the Tracking Technologies, Lenovo enabled comprehensive data collection regarding users' communications and personal identifiers covered by the DOJ Rule so that it could then share that information with entities covered under the DOJ Rule, including the Lenovo Group.

---

[8] Lenovo.com December 2025 Traffic Stats, *available at* https://www.semrush.com/website/lenovo.com/overview/ (last visited Jan. 27, 2026).

68. This is significant because, in the hands of a foreign adversary, the data intercepted by the Tracking Technologies can be used for far more than just e-commerce.

69. A company like the Lenovo Group, operating under Chinese jurisdiction, can use this data to build detailed dossiers on U.S. residents, identify psychological or financial vulnerabilities, and target individuals in sensitive roles—such as jurists, military personnel, journalists, politicians, or dissidents.

70. This data can be weaponized for profiling, coercive targeting, or even blackmail, all without the user's knowledge that their information is being transmitted to a foreign-controlled entity.

71. Indeed, such vulnerabilities prompted the passage of the DOJ Rule in the first place.[9]

D. LENOVO KNOWINGLY VIOLATES THE DOJ RULE.

72. On April 8, 2025, the U.S. Department of Justice issued the DOJ Rule, codified at 28 C.F.R. Part 202, to restrict the transfer of Americans' bulk sensitive personal data to "countries of concern," including China.

73. Under the DOJ Rule, it is unlawful to transfer "bulk U.S. sensitive personal data"—including the categories of persistent identifiers that Lenovo obtains from the Tracking Entities—to certain entities associated with adversarial foreign governments.

74. Lenovo has long been recognized as a national security threat.

75. In 2016, the U.S. Department of Defense's Joint Staff issued a warning that Lenovo computers and devices could introduce compromised hardware into defense supply chains, posing cyber espionage risks.[10]

---

[9] Justice Department Issues Final Rule Addressing Threat Posed by Foreign Adversaries' Access to Americans' Sensitive Personal Data *available at* https://www.justice.gov/archives/opa/pr/justice-department-issues-final-rule-addressing-threat-posed-foreign-adversaries-access (last visited Jan. 27, 2026).

[10] Scott Nicholas, *DoD Joint Staff Issues Cybersecurity Warning Against Lenovo Computers, Handheld Devices*, ExecutiveGov *available at* https://www.executivegov.com/articles/dod-joint-staff-issues-cybersecurity-warning-against-lenovo-computers-handheld-devices (last visited January 29, 2026).

76. Similar concerns were raised in Pentagon and watchdog reports about such risks.[11]

77. In 2023, members of the U.S. House Select Committee on the Chinese Communist Party raised questions about Lenovo's ties to the Chinese government, citing its well documented links to state-run cyberespionage campaigns.[12]

78. Lenovo admits in its Website's Privacy Policy that it transfers users' personal information to the Lenovo Group and the People's Republic of China.[13]

79. Further, the Website's Privacy Policy purports to safeguard personal information transferred to China only by maintaining agreements and standard contractual clauses that govern the transfer, processing and protection of personal information.[14]

80. However, under the DOJ Rule, a U.S. entity that engages in a restricted covered data transaction must do more than maintain agreements and standard contractual clauses—it must ensure the bulk U.S. data is not transferred to countries of concern—by implementing detailed security controls and documentation covering data access protections, segmentation, auditing, and restrictions on onward transfer to covered persons.

81. This is not inadvertent—Lenovo is aware of the requirements of the DOJ Rule.

82. Indeed, Lenovo is a member of industry groups, including the Information Technology Industry Council ("ITI") that actively participated in the DOJ Rulemaking process

---

[11] Roslyn Layton, *New Pentagon Report Shows How Restricted Chinese IT Products Routinely Enter US Military Networks*, American Enterprise Institute - AEI *available at* https://www.aei.org/technology-and-innovation/new-pentagon-reports-shows-how-restricted-chinese-it-products-routinely-make-their-way-into-us-military-networks/

[12] Letter From Select Committee on Chinese Communist Party, *available at* https://chinaselectcommittee.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/10.04.2023-letter-to-navy-exchange.pdf (last visited January 29, 2026).

[13] Lenovo Privacy Statement | Lenovo US *available at* https://www.lenovo.com/us/en/privacy/ (last visited January 29, 2026).

[14] *Id.*

leading to the U.S. Department of Justice's adoption of the DOJ Rule in April 2025.[15]

83. In public comment letters submitted to DOJ, the ITI specifically requested that the DOJ "exempt any data that is processed by a covered person on behalf of a U.S. person if: (i) the purpose of the processing is product research, development, or improvement; (ii) the U.S. person directs and controls the manner of processing the data; and (iii) the covered person is contractually bound by the U.S. person to maintain the privacy and security of the data."[16]

84. However, the DOJ ultimately did not adopt that exemption.[17]

85. Nonetheless, Lenovo's Privacy Policy concedes that it transfers users' personal information to the Lenovo Group and the People's Republic of China and only safeguards such information by maintaining agreements and standard contractual clauses that govern the transfer, processing and protection of personal information—effectively admitting that Lenovo knowingly engages in practices that violate the DOJ Rule.

86. Lenovo's awareness of this legal risk is further reflected in corporate disclosures.

87. For example, in recent annual reports, the Lenovo Group recognized "[t]he risk that there are instances of non-compliant collection, processing, use, retention, sharing, cross-border transfer, and protection of proprietary, confidential, and personal (customer, supplier, employee), user or device-identifiable data, leading to violations of applicable privacy, security, and data protection laws and regulations."[18]

88. It also acknowledged that "Lenovo [Group] collects and manages personally identifiable information (PII) and other sensitive data across its global operations. The Group is

---

[15] Members - Information Technology Industry Council *available at* https://www.itic.org/about/membership/iti-members (last visited January 29, 2026).

[16] ITI Comment to U.S. Department of Justice ANPRM: Provisions Pertaining to Preventing Access to Americans' Bulk Sensitive Personal Data and Government-Related Data by Countries of Concern, Docket No. NSD 104, April 19, 2024.

[17] 28 CFR §§ 202.501-202.511, 202.801-202.803 (listing exemptions adopted).

[18] Lenovo Group 2023 Annual Report *available at* https://doc.irasia.com/listco/hk/lenovo/annual/2023/ar2023.pdf (last visited January 29, 2026).

subject to a range of data privacy laws and security regulations that govern the collection, use, cross-border transfer, and retention of such information."[19]

89. Despite the DOJ's clear guidance, Lenovo has continued to transmit sensitive user data to China.

90. These transmissions include identifiers covered by the DOJ Rule, browsing behavior, and contextual metadata that enable Lenovo, and its foreign parents, to track, profile, and retain data about U.S. residents.

91. Lenovo's conduct is not accidental, peripheral, or the result of isolated technical missteps.

92. Rather, Lenovo knowingly facilitated the export of Americans' behavioral data to a foreign adversary.

93. In doing so, it disregarded binding federal law, the DOJ Rule, created specifically to address what the U.S. government has called an "unusual and extraordinary threat" to the national security and foreign policy of the United States.

E. FACTS SPECIFIC TO REPRESENTATIVE PLAINTIFF.

94. Plaintiff Spencer Christy is a resident of San Francisco, California.

95. In November and December of 2025, Plaintiff visited the Website on multiple occasions.

96. During these visits to the Website, Plaintiff navigated multiple product pages utilizing full-string URLs displaying the product viewed and displaying that he was searching for a discounted gaming computer.

97. Plaintiff also searched the Website for, *inter alia*, the Legion Tower 7i Gen 10 (Intel) with RTX™ 5080, which he ultimately purchased.

98. While Plaintiff was actively viewing the Website, his browser loaded code implemented by Defendant and operated by the Tracking Technologies.

99. This code initiated automated requests sent from Plaintiff's browser to third party

[19] Lenovo Group 2025 Annual Report *available at* https://doc.irasia.com/listco/hk/lenovo/annual/2025/ar2025.pdf (last visited January 29, 2026).

servers and triggered the interception of his data.

100. Those requests featured persistent identifiers uniquely associated with Plaintiff—including his cookie IDs, device IDs, IP addresses, and browser metadata—along with the full URL of the specific page that Plaintiff was viewing at the time, which displayed the specific product he was viewing, and displayed that he was searching for a discounted gaming computer.

101. Defendant then used these intercepted communications for its own purposes, including enriching persistent profiles and databases which were then transferred to, or accessible by, its parent company, the Lenovo Group, in direct violation of the DOJ Rule. Indeed, Lenovo admits in the Website's Privacy Policy that Lenovo transfers users' personal information within the Lenovo Group to the People's Republic of China without the requisite safeguards and controls.[20]

102. As a result, the Lenovo Group, a covered person under the DOJ Rule, received detailed information about Plaintiff's online behavior and interests, without his knowledge or consent.

103. Lenovo's covert tracking and sharing of Plaintiff's sensitive data violates his reasonable expectation of privacy.

104. This data, particularly when appended to persistent profiles, reveals sensitive details about Plaintiff. Aggregating and utilizing this information without Plaintiff's knowledge or consent goes far beyond what any reasonable consumer would expect and constitutes a serious intrusion into private life.

105. Plaintiff did not consent to the interception, enrichment, or foreign transmission of his browsing data.

106. Lenovo's conduct caused Plaintiff concrete and particularized harm, including the unauthorized disclosure of personal information to a foreign entity, the invasion of his privacy, and the loss of control over how and where his browsing behavior was used and shared.

//

//

//

[20] *See, supra*, n.13.

CLASS ALLEGATIONS

107. Plaintiff brings this proposed class action lawsuit pursuant to Federal Rule of Civil Procedure 23(b)(2) and Rule 23(b)(3) on behalf of himself and a Class (the "Class"), a California subclass (the "California Subclass") and a California purchaser subclass (the "California Purchaser Subclass" and together with the Class and the California Subclass, the "Classes") of all others similarly situated, defined as follows:

a. **Nationwide Class**: All individuals in the United States whose electronic communications with the Website were intercepted and whose communications and personal data—including persistent identifiers and behavioral activity—was used on or after April 8, 2025.

b. **California Subclass**: All individuals who resided in the State of California at the time their electronic communications with the Website were intercepted.

c. **California Purchaser Subclass**: All members of the California Subclass who resided in the State of California and made purchases on the Website and had electronic communications with the Website intercepted.

108. Excluded from the Classes are: (i) any Judge or Magistrate presiding over this action and members of their families; (ii) Defendant, Defendant's subsidiaries, parents, successors, predecessors, and any entity in which Defendant or its parents have a controlling interest and its officers and directors; (iii) persons who properly execute and file a timely request for exclusion from the Class; (iv) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (v) Plaintiff's counsel and Defendant's counsel; and (vi) the legal representatives, successors, and assigns of any such excluded persons.

109. **Numerosity**: The exact number of Subclasses members is unknown and not available to Plaintiff at this time, but individual joinder is impracticable. On information and belief, Defendant has many thousands of users who fall into the definition of the Class and Subclass. Subclasses members can be identified through Defendant's records.

110. **Commonality and Predominance**: There are questions of law and fact common to the claims of Plaintiff and the alleged Classes, and those questions predominate over any questions that may affect individual members of the Classes. Common questions for the Classes members

include, but are not necessarily limited to the following:

a. Whether Defendant used tracking technologies to cause users' web browsers to reroute electronic communications—including URLs, metadata, and behavioral activity;

b. Whether Defendant used a device, as defined under 18 U.S.C. § 2510(5), to intercept the contents of communications from Plaintiff and the Class;

c. Whether Defendant obtained valid consent from Plaintiff and the Class to aid in the interception and disclosure their electronic communications to third parties, and to use such communications;

d. Whether the data transmitted by Defendant constitutes "bulk U.S. sensitive personal data" under the DOJ Rule;

e. Whether Defendant's transmission of data to its Chinese-controlled entities constitutes a prohibited or restricted transaction under the DOJ Rule;

f. Whether Defendant acted knowingly and with intent to share the information;

g. Whether Defendant's interception and disclosure of users' communications falls within the crime-tort exception to the ECPA's party-consent provision;

h. Whether Defendant was unjustly enriched at the expense of the Class;

i. Whether Defendant's actions violate California laws invoked herein; and

j. Whether Plaintiff and Class members are entitled to damages, restitution, injunctive and other equitable relief, reasonable attorneys' fees, prejudgment interest and costs of this suit.

111. **Typicality**: Plaintiff's claims are typical of the claims of members of the Class and Subclass. The claims arise from a common nucleus of operative fact—inter alia, the surreptitious interception and illicit transfer of their personal information to a foreign adversary of the United States. Plaintiff, like all members of the Class and Subclass, had his information unlawfully intercepted and has been injured by Defendant's misconduct at issue.

112. **Adequate Representation**: Plaintiff will fairly and adequately represent and protect the interests of the Classes and has retained counsel competent and experienced in complex litigation and class actions. Plaintiff's claims are representative of the claims of the other members of the Class and Subclass. That is, Plaintiff and the members of the Classes sustained injuries and damages as a result of Defendant's conduct. Plaintiff also has no interests antagonistic to those of the Class or Subclass, and Defendant has no defenses unique to Plaintiff. Plaintiff and her counsel

are committed to vigorously prosecuting this action on behalf of the members of the Classes and have the financial resources to do so. Neither Plaintiff nor their counsel have any conflicts with or interests adverse to the Class or Subclass.

113. **Superiority**: Class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy, as joinder of all members of the Classes is impracticable. Individual litigation would not be preferable to a class action because individual litigation would increase the delay and expense to all parties due to the complex legal and factual controversies presented in this Complaint as well as the risk of inconsistent adjudication. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court. Through a class action, economies of time, effort, and expense will be fostered, and uniformity of decisions will be ensured.

114. Plaintiff reserves the right to revise the foregoing "Class Allegations" and "Class Definitions" based on facts learned through additional investigation and in discovery.

TOLLING, CONCEALMENT, AND ESTOPPEL

115. The applicable statutes of limitations have been tolled by Defendant's knowing and active concealment and denial of the facts alleged herein.

116. Defendant affirmatively hid its true actions and knowingly made statements that were misleading and concealed the true nature of their conduct and operation.

117. The circumstances of the third-party Tracking Technologies use on Defendant's Website would lead reasonable users to believe third parties were not collecting their information or that Defendant was facilitating disclosure of the same.

118. Moreover, Plaintiff was ignorant of the information essential to pursue his claims, without any fault or lack of diligence on his own part.

119. Furthermore, under the circumstances Defendant was under a duty to disclose the true character, quality, and nature of its activities to Plaintiff. Defendant therefore is estopped from relying on any statute of limitations.

120. All applicable statutes of limitation also have been tolled by operation of the

discovery rule. Specifically, Plaintiff and other Class members could not have learned through the exercise of reasonable diligence of Defendant's conduct as alleged herein.

121. Accordingly, Plaintiff and the Class members could not have reasonably discovered the truth about Defendant's practices until shortly before this class litigation was commenced.

CAUSES OF ACTION

FIRST CAUSE OF ACTION

VIOLATIONS OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT
18 U.S.C §2510, *et seq.*
(*On Behalf of Plaintiff & the Nationwide Class*)

122. Plaintiff repeats and re-alleges all factual allegations contained in the foregoing paragraphs as if fully set forth herein.

123. Plaintiff brings this claim individually and on behalf of the members of the Nationwide Class against Defendant.

124. The ECPA prohibits any person from "intentionally intercept[ing], endeavor[ing] to intercept, or procur[ing] any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication." 18 U.S.C. § 2511(1)(a).

125. The ECPA also prohibits any person from "intentionally us[ng], or endeavor[ing] to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication." 18 U.S.C. § 2511(1)(d).

126. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire, oral, or electronic communication is intercepted or used in violation of 18 U.S.C § 2511.

127. Defendant knowingly and intentionally distributes and maintains the Tracking Technologies on the Website for the purpose of rerouting user communications to the Tracking Technologies' servers for Defendant's later use.

128. The Tracking Technologies intentionally capture the contents of users' interactions with the Website and purposefully transmit them to the Tracking Technologies' servers.

129. The Tracking Technologies' tracking code executed automatically within Plaintiff's

and Nationwide Class members' browsers during the page load process without Plaintiff's consent.

130. This code intercepted the contents of Plaintiff's and Nationwide Class members' interactions with the Website by rerouting their communications—including but not limited IP addresses, identifiers, full URLs, page titles, and the content of the page—to the Tracking Technologies.

131. These interceptions occurred as part of the browser's rendering of the Website, before Plaintiff or members of the Nationwide Class could detect the transmissions or consent to the transmissions.

132. When Plaintiff and the Nationwide Class members navigate the Website, the Tracking Technologies' code causes their browsers to transmit IP addresses, identifiers, full URLs, page titles, related to Plaintiff and the Nationwide Class members in real time.

133. These transmissions occur without the user's awareness or consent and are initiated automatically during the same browser session in which the user communicates with the Website.

134. The Tracking Technologies' capture of these communications constitutes an unlawful interception under the ECPA. Defendant's subsequent use of these communications constitutes an unlawful use under the ECPA.

135. **Contents of a Communication:** The data intercepted by the Tracking Technologies from Plaintiff and members of the Nationwide Class includes full-page URLs and identifiers. These qualify as the "contents" of a communication under 18 U.S.C. § 2510(8) because they reveal the substance and subject matter of the user's communications with the Website.

136. **Use of a Device:** The technologies the Tracking Technologies use to intercept this data—including but not necessarily limited to web beacons, pixels, software development kits, APIs, JavaScript, real-time bidding and other scripts, and cookies—constitute "devices" under 18 U.S.C. § 2510(5), which includes any device or apparatus used to intercept electronic communications.

137. **Lack of Consent:** Plaintiff and Nationwide Class members did not consent to the Tracking Technologies' interception or disclosure of their communications.

138. The Website did not provide clear or conspicuous notice that user interactions would

be surveilled and routed to foreign entities, and Plaintiff and Nationwide Class members lacked a reasonable means to opt out of the Tracking Technologies' data collection and sharing. There was no actual or implied consent under applicable law.

139. **Crime-Tort Exception:** The "party exception" in 18 U.S.C. § 2511(2)(d) does not apply. At the time of the interception, the Tracking Technologies' interception and, and Defendant's use of these communications, was undertaken knowingly and intentionally for the purpose of committing a criminal and tortious act—namely, the unlawful transmission of bulk U.S. sensitive personal data to a covered foreign entity in violation of the Rule, 28 C.F.R. Part 202.

140. On or after April 8, 2025, Defendant knowingly engaged in prohibited or restricted data transactions with the Lenovo Group, a foreign-owned entity, organized under the laws of Hong Kong, with its principal place of business in China, without the requisite security requirements, in violation of the Rule. 28 C.F.R. §§ 202.301, 202.401.

141. Defendant is a corporation organized and existing under the laws of the State of Delaware, with its principal place of business located in North Carolina. Because Defendant is organized under the laws of the United States and is an entity in the United States, Defendant is a "U.S. person" under 28 C.F.R. § 202.256.

142. The Lenovo Group qualifies as a "covered person" under 28 C.F.R. § 202.211(a) because it is a Chinese company with substantial operations and executive oversight in the People's Republic of China—a "country of concern" under the Rule.

143. The Lenovo Group maintains a significant presence in China and is subject to Chinese law, including China's National Intelligence Law, Cybersecurity Law, and Data Security Law.

144. These laws compel Chinese companies and individuals to secretly cooperate with government surveillance efforts and grant authorities unrestricted access to private user data.

145. The Lenovo Group's operations are subject to Chinese government control, oversight, and compelled disclosure obligations.

146. The Tracking Technologies initiate requests which result in the transmission of numerous protected "listed identifiers" under the Rule, including but not limited to IP addresses

(28 C.F.R. § 202.234(g)), advertising IDs (28 C.F.R. § 202.234(e)), and cookie data (28 C.F.R. § 202.234(g)) to and through the Tracking Technologies' and into Defendant's possession.

147. Defendant then transmits or provides access to these protected identifiers together, including, for example, transmitting a given user's IP address along with the user's cookie data and advertising IDs, such that the identifiers are clearly linked with one another and are associated or reasonably capable of being associated with each related user to the Lenovo Group.

148. This information qualifies as "covered personal identifiers" and "sensitive personal data" under the DOJ Rule because these identifiers are shared with the Lenovo Group (i) in combination with at least one other listed identifier, or (ii) in combination with other data such that the listed identifier is or can reasonably be associated with other listed identifiers or other sensitive personal data. *See* 28 C.F.R. §§ 202.212(a), 202.249(a).

149. On information and belief, Lenovo has collected or maintained this sensitive personal data relating to more than 100,000 U.S. persons (including Plaintiff and Nationwide Class members) following the effective date of the DOJ Rule, and therefore this information constitutes "bulk U.S. sensitive data" under 28 C.F.R. § 202.206.

150. Indeed, publicly available web traffic reports estimate that 13.35 million U.S.-based devices visited the Website in December of 2025, alone.[21]

Defendant provides this data to the Lenovo Group. Indeed, Lenovo admits in the Website's Privacy Policy that Lenovo transfers users' personal information within the Lenovo Group and to the People's Republic of China, without the requisite safeguards and security controls. Lenovo's provision of this bulk U.S. sensitive data to the Lenovo Group, a covered person, constitutes a covered data transaction involving data brokerage under 28 C.F.R. §§ 202.210, 202.214, 202.301, 202.401.

151. Defendant is a member of industry associations that directly participated in the Rule rulemaking process that publicly warned members of the legal risks of transmitting certain data to entities based in China.

152. Lenovo also acknowledged in its own regulatory filings that it is at risk of violating

[21] *See, supra*, n.8.

privacy and data transfer regulations.

153. For these reasons, Lenovo knew or reasonably should have known that it had engaged and was engaging in covered data transactions involving data brokerage in violation of the DOJ Rule.

154. Because Lenovo knowingly engaged and engages in covered data transactions with Lenovo Group, a covered person, Lenovo has violated the DOJ Rule's prohibition of data-brokerage transactions under 28 C.F.R. § 202.301 and/or of engaging in restricted transactions without the requisite security controls under 28 C.F.R. § 202.401.

155. In addition to Lenovo's tortious and criminal intent to violate the DOJ Rule by sharing certain information with entities subject to the jurisdictional control of China, as described further below, the interceptions by the Tracking Technologies were also knowingly and intentionally performed for the independent purpose of committing tortious acts in violation of California common law, specifically:

a. Violating Plaintiff's and the California Subclass members' right to privacy conferred by the California Constitution through the creation and dissemination of highly detailed identity profiles, enriched by the contents of Plaintiff's and the California Subclass members' communications intercepted by the Tracking Technologies, as described herein; and

b. Committing the tort of intrusion upon seclusion under California common law by using the contents of the intercepted communications to facilitate the creation of highly detailed identity profiles on Plaintiff and Class members, which were then used and disseminated as described herein.

156. Because the Tracking Technologies intentionally and knowingly intercepted and disclosed, and Defendant intentionally and knowingly used Plaintiff's and Classes members' communications for the purpose of committing these criminal and tortious acts, it is not shielded by the "party exception" under the ECPA.

157. Plaintiff and the Class suffered harm as a result of Defendant's violations of the ECPA, including the transmission of their sensitive data to a foreign adversary, and therefore seek (a) preliminary, equitable, and declaratory relief as may be appropriate, (b) the sum of the actual damages suffered and disgorgement of profits obtained by Defendant as a result of its unlawful conduct, or statutory damages as authorized by 18 U.S.C. § 2520(c)(2), whichever is greater, (c) punitive damages, and (d) reasonable costs and attorneys' fees.

158. Plaintiff, individually and on behalf of the Nationwide Class members, seeks all monetary and non-monetary relief allowed by law, including actual damages, statutory damages, punitive damages, preliminary and other equitable or declaratory relief, and attorneys' fees and costs.

SECOND CAUSE OF ACTION

CALIFORNIA INVASION OF PRIVACY ACT
Cal. Penal Code § 631, *et seq.*
(*On Behalf of Plaintiff & the California Subclass*)

159. Plaintiff repeats and re-alleges all factual allegations contained in the foregoing paragraphs as if fully set forth herein.

160. Plaintiff brings this claim individually and on behalf of the members of the California Subclass.

161. The California Invasion of Privacy Act ("CIPA") is codified at Cal. Penal Code §§ 630 to 638.

162. The Act begins with its statement of purpose: "The Legislature hereby declares that advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping on private communications and the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society." Cal. Penal Code § 630.

163. California Penal Code § 631(a) provides in relevant part:

> any person who, by means of any machine, instrument, or contrivance, or in any other manner … willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable by a fine not exceeding two thousand five hundred dollars ($2,500).

164. A defendant must show it had the consent of all parties to the communication.

165. At all relevant times, Defendant aided, agreed with, and conspired with third parties to track and intercept Plaintiff's and the California Class members' internet communications exchanged with Defendant while accessing Defendant's website. Defendant assisted these interceptions without the requisite consent from Plaintiff and the California Class members.

166. The Tracking Technologies intercepted these communications without consent from all parties to the communications.

167. The Tracking Technologies intended to learn, and did learn, some meaning of the content in the communications including without limitation in the URLs, search queries, and other content described herein exchanged between the California Class members and Defendant on Defendant's Website.

168. Defendant, when aiding and assisting Tracking Technologies' eavesdropping, intended those third parties to learn the content of the visitor's communications.

169. Defendant used, or attempted to use, information so obtained or, in the alternative, aided and assisted the Lenovo Group in using or attempting to use, information so obtained.

170. The following items constitute "machine[s], instrument[s], or contrivance[s]" under the CIPA, and, even if they do not, the tracking technology provided by the third parties falls within the broad catch-all category of "any other manner":

a. The computer codes and programs that the Tracking Technologies used to track Plaintiff's and the Class members' communications while they navigated the Website;

b. Plaintiff's and Class members' browsers;

c. Plaintiff's and Class member's computing and mobile devices;

d. The web and ad servers of the Tracking Technologies;

e. The computer codes and programs that the Tracking Technologies used to track and intercept the Plaintiff's and Class members' communications while they were using a browser to visit Defendant's Website.

171. The tracking and interception of Plaintiff's and Class members' communications while they were using a web browser or mobile application to visit Defendant's Website originated in and was executed in California.

172. Pursuant to California Penal Code § 637.2, Plaintiff and the California Class members have been injured by the violation of California Penal Code § 631 and each seek damages for the greater of $5,000 or three times the actual amount of damages, as well as injunctive relief.

THIRD CAUSE OF ACTION

CALIFORNIA INVASION OF PRIVACY ACT
Cal. Penal Code § 632, *et seq.*
(On Behalf of Plaintiff & the California Subclass)

173. Plaintiff repeats and re-alleges all factual allegations contained in the foregoing paragraphs as if fully set forth herein.

174. Plaintiff brings this claim individually and on behalf of the members of the California subclass against Defendant.

175. California Penal Code Section 632(a) provides that:

> [E]very person who, intentionally and without the consent of all parties to a confidential communication, uses an electronic amplifying or recording device to eavesdrop upon or record the confidential communication, whether the communication is carried on among the parties in the presence of one another or by means of a telegraph, telephone, or other device, except a radio, shall be punished[.]

176. The data collected on Defendant's Website constitutes "confidential communications," as that term is used in Section 632, because class members had an objectively reasonable expectation of privacy in the circumstances.

177. Defendant intentionally used an electronic recording device—specifically, the tracking technology embedded within the Website—to eavesdrop upon and record these confidential communications.

178. This technology constitutes an "electronic amplifying or recording device" within the meaning of Section 632(a) because it is specifically designed to capture, record, and transmit user interactions and communications in real-time for analytics and behavioral tracking purposes.

179. Defendant intentionally implemented and activated this recording technology within its Website with full knowledge that it would capture and record users' confidential communications.

180. Defendant's recording of Plaintiff's and California Subclass members' confidential communications was accomplished without the requisite consent.

181. Defendant's conduct was undertaken intentionally and with knowledge that the Tracking Technologies would record confidential communications without the requisite consent.

182. The confidential communications that were unlawfully recorded include protected information that individuals provided with reasonable expectations of confidentiality.

183. Defendant is directly liable under section 632. Alternatively, Defendant is liable for aiding in violations of section 632 by the Tracking Technologies and/or the Lenovo Group.

184. As a direct and proximate result of Defendant's violations of Section 632, Plaintiff and the California Subclass members have suffered harm including invasion of their privacy rights, violation of confidentiality and protection by the DOJ Rule, and loss of control over their sensitive information.

185. Unless enjoined and restrained by this Court, Defendant will continue to commit these violations. Plaintiff and Class members have a reasonable fear that their confidential communications will continue to be unlawfully recorded if they use the Website.

186. Pursuant to Cal. Penal Code § 637.2, Plaintiff and the California Class members have been injured by the violations of Cal. Penal Code § 632, and each seek damages for the greater of $5,000 or three times the amount of actual damages, as well as injunctive relief.

FOURTH CAUSE OF ACTION

UNJUST ENRICHMENT
(*On Behalf of Plaintiff & the Nationwide Class*)

187. Plaintiff repeats and re-alleges all factual allegations contained in the foregoing paragraphs as if fully set forth herein.

188. Plaintiff brings this claim individually and on behalf of the members of the Nationwide Class against Defendant.

189. Defendant has been unjustly enriched at the expense of Plaintiff and Class members through its unauthorized collection, use, and monetization of their personal data.

190. Plaintiff and Class members conferred benefit upon Defendant by providing

valuable information through their use of the Website.

191. Such sensitive information commands exceptional value due to its predictive power and marketing utility.

192. Defendant received and retained this benefit by intercepting, collecting, and transmitting Plaintiff's and Class members' sensitive to the Tracking Technologies and the Lenovo Group through embedded technology without authorization or consent.

193. Defendant has been unjustly enriched through several mechanisms:

a. **Data Monetization:** Defendant derives commercial value from sharing users' information with third parties for marketing analytics, behavioral targeting, and user profiling purposes;

b. **Cost Avoidance:** Defendant avoided the substantial costs of obtaining proper consent, implementing adequate privacy protections, and securing lawful access to this valuable data;

c. **Competitive Advantage:** Defendant gained unfair competitive advantages by leveraging detailed data profiles to optimize its platform and marketing without bearing the costs associated with compliant data collection.

d. **Enhanced Platform Value:** The unauthorized collection of comprehensive user data increases the overall value and effectiveness of Defendant's platform, and the PRC's surveillance apparatus.

194. Defendant obtained this benefit through unlawful interception and unauthorized disclosure of information in violation of the DOJ Rule, ECPA, Cal. Penal Code §§ 631-632, and/or the CDAFA.

195. Whereas Plaintiff and Class members provided this valuable information with a reasonable expectation of privacy and DOJ Rule compliance, Defendant actively concealed its data collection and sharing practices from users who were unaware their sensitive information was being intercepted and monetized.

196. Defendant's retention of these benefits violates fundamental principles of fairness and equity, as Defendant has profited from the unauthorized exploitation of sensitive and valuable

personal information without providing any compensation or benefit to the individuals whose privacy was violated.

197. Plaintiff and Class members have no adequate remedy at law for Defendant's Unjust Enrichment, as they cannot recover the specific value of their appropriated data through traditional damages calculations.

198. As a direct and proximate result of Defendant's Unjust Enrichment, Plaintiff and Class members are entitled to restitution and disgorgement of all benefits, profits, and value that Defendant has obtained through the unauthorized collection and use of their protected information.

199. Plaintiff and Class members seek judgment requiring Defendant to disgorge all profits, benefits, and value obtained through its unlawful conduct, together with interest thereon, and such other relief as the Court deems just and proper.

FIFTH CAUSE OF ACTION

INVASION OF PRIVACY
(*On Behalf of Plaintiff & the California Class*)

200. Plaintiff repeats and re-alleges all factual allegations contained in the foregoing paragraphs as if fully set forth herein.

201. Plaintiff brings this claim individually and on behalf of the members of the California Class against Defendant.

202. The right to privacy in California's constitution creates a right of action against private entities such as Defendant.

203. Plaintiff's and Class members' expectation of privacy is deeply enshrined in California's Constitution.

204. Article I, section 1 of the California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among those are enjoying and defending life and liberty, acquiring, possessing, and protecting property and obtaining safety, happiness, and private."

205. The phrase "and privacy" was added in 1972 after voters approved a proposed legislative constitutional amendment designated as Proposition 11.

206. Critically, the argument in favor of Proposition 11 reveals the legislative intent was to curb business' control over unauthorized collection and use of consumers' personal information:

> The right of privacy is the right to be left alone ... It prevents government and business interests from collecting and stockpiling unnecessary information about us and from misusing information gathered for one purpose in order to serve other purposes or to embarrass us. Fundamental to our privacy is the ability to control circulation of personal information. This is essential to social relationships and personal freedom.

207. The principal purpose of this constitutional right was to protect against unnecessary information gathering, use, and dissemination by public and private entities, including Defendant.

208. Plaintiff and the California Subclass members have a legally protected interest in preventing the unauthorized collection, aggregation, and dissemination of their personal information, particularly when this data reflects sensitive aspects of their personal lives.

209. Plaintiff and the California Subclass also have a strong interest in preventing the widespread distribution of detailed behavioral profiles to unknown third parties—including foreign entities—without their knowledge or consent.

210. Plaintiff and the California Subclass maintain a reasonable expectation of privacy in their day-to-day lives, including in their Internet browsing activity, online communications, and the personal data that Defendant surreptitiously collects, enriches, and shared with countries of concern without the knowledge or consent of Plaintiff and the California Subclass members.

211. Defendant invades these interests, in violation of Plaintiff's and the California Subclass members' reasonable expectation of privacy through its covert collection, aggregation, correlation, and dissemination of sensitive information and persistent identifiers tied to Plaintiff and the California Subclass members as alleged herein.

212. Defendant intentionally and extensively violates the reasonable expectation of privacy held by Plaintiff and the California Subclass members through engaging in this covert, large-scale data collection, designed to uniquely identify and surveil individuals.

213. This extensive covert surveillance and targeting would be highly offensive to a reasonable person and constitutes an egregious breach of social norms.

214. Defendant stockpiles a vast range of personal information, including persistent

identifiers (e.g., cookie IDs, device IDs, mobile advertising IDs, and IP addresses), device metadata (e.g., screen resolution, browser version, operating system, and language settings), and contextual information such as full URLs and referring pages. This contextual data often reveals the exact content being viewed by the individual.

215. This widespread surveillance and distribution of personal data occurs without meaningful disclosure or the requisite consent and defies users' reasonable expectations of privacy. No reasonable user would expect that Lenovo would collect and distribute sensitive information to countries of concern.

216. Secretly collecting such data in sensitive contexts is highly offensive. Correlating that information into detailed user profiles is highly offensive. Sharing those profiles with a foreign adversary is highly offensive.

217. As described above, the U.S. government has identified China and its control of personal data as adversarial to national security and the safety of U.S. citizens.

218. Americans have a strong interest in protecting their personal data from an entity the U.S. government has identified as a threat to national security and the safety of U.S. citizens.

219. Despite the dangers of sharing this sensitive data with a company subject to Chinese control, Lenovo knowingly shares sensitive information with the Lenovo Group.

220. These actions represent egregious breaches of social norms and violate both the reasonable expectation of privacy held by Plaintiff and the California Subclass members, and the constitutional right to privacy guaranteed under California law.

221. In short, committing criminal and tortious acts against millions of Americans constitutes an egregious breach of social norms that is highly offensive.

222. As a result of these extensive and intentional invasions of privacy, Plaintiff and the California Subclass members have suffered harm and are entitled to compensation and injunctive relief.

//

//

//

SIXTH CAUSE OF ACTION

INTRUSION UPON SECLUSION UNDER CALIFORNIA COMMON LAW
(*On behalf of Plaintiff & the California Subclass*)

223. Plaintiff and the California Subclass members incorporate the foregoing allegations as if fully set forth herein.

224. Plaintiff and the California Subclass members have a strong interest in preventing the unauthorized collection, aggregation, and dissemination of their personal information.

225. These individuals maintain a reasonable expectation of privacy in their day-to-day lives—an expectation that extends not only to their Internet browsing activity and online communications, but also to the personal data that Lenovo surreptitiously collects, enriches, de-anonymizes, and shares with covered persons without the knowledge or consent of Plaintiff and the California Subclass members.

226. Lenovo has violated Plaintiff's and the California Subclass members' reasonable expectation of privacy through its collection, aggregation, correlation, and dissemination of Plaintiff's and the California Subclass members' personal information.

227. Lenovo's practices are highly offensive to a reasonable person and constitute an egregious breach of social norms.

228. Lenovo intentionally and extensively violates the reasonable expectation of privacy held by Plaintiff and the California Subclass members through engaging in covert, large-scale data collection designed to uniquely identify and surveil U.S. individuals.

229. Lenovo uses tools that secretly harvest and correlate personal information, enriches that data with additional details, and builds highly detailed identity profiles unique to each individual.

230. These profiles are then shared with the Lenovo Group and other covered persons.

231. Collecting detailed information about a person's device, behavior, or website usage is inherently intrusive.

232. Most people would be shocked to learn that simply opening the Website could trigger data harvesting and the silent creation of a detailed behavioral profile tied to their identity.

233. This covert surveillance, subsequent profiling, and onward sharing with foreign adversaries, would be highly offensive to a reasonable person and constitutes a profound violation of social norms.

234. Lenovo, through the Tracking Technologies, does not merely collect isolated data points from Plaintiff and California Subclass members. It stockpiles a vast range of personal information, including persistent identifiers (e.g., cookie IDs, device IDs, mobile advertising IDs, and IP addresses), device metadata (e.g., screen resolution, browser version, operating system, and language settings), and contextual information such as full URLs and referring pages. This contextual data often reveals the exact content being viewed by the individual.

235. Through these practices, Lenovo aids the interception, tracks, collects, aggregates, uses, and redistributes the Internet activity and communications of Plaintiff and Subclass members.

236. Lenovo's extensive use of identifying cookies further enable the linkage of user identifiers across sessions, allowing Lenovo to build a detailed, persistent profile on each individual.

237. Correlating this data into rich behavioral profiles, then attaching persistent identifiers that allow parties to link the behavior to real-world identities is also highly offensive to a reasonable person. Moreover, sharing those profiles with foreign adversaries, without the user's knowledge or meaningful consent, is highly offensive behavior.

238. As described above, the U.S. government has identified China and its control of personal data as adversarial to national security and the safety of U.S. citizens. Americans have a strong interest in protecting their personal data from an entity the U.S. government has identified as a threat to national security and the safety of U.S. citizens.

239. Despite the dangers of sharing this sensitive data with a company subject to Chinese control, Lenovo knowingly shares sensitive information—including browsing activity, behavioral insights, and personal identifiers—with countries of concern.

240. The extent of Lenovo's collection, enrichment, and redistribution of highly detailed identity profiles is staggering and highly offensive.

241. These actions represent egregious breaches of social norms and violate the

reasonable expectation of privacy held by Plaintiff and the California Subclass members.

242. Lenovo lacks any legitimate business interest in covertly tracking, profiling, and aggregating the identities and private information of Plaintiff and the California Subclass members.

243. As a result of these extensive and intentional invasions of privacy, Plaintiff and the California Subclass members have suffered harm and are entitled to just compensation and injunctive relief.

SEVENTH CAUSE OF ACTION

VIOLATION OF THE COMPREHENSIVE COMPUTER DATA AND ACCESS AND FRAUD ACT
Cal. Penal Code § 502, *et seq.*
(*On behalf of Plaintiff & the California Subclass*)

244. Plaintiff and the California Subclass members incorporate the foregoing allegations as if fully set forth herein.

245. California's Comprehensive Data and Access and Fraud Act ("CDAFA") provides: "For purposes of bringing a civil or a criminal action, a person who causes, by any means, the access of a computer, computer system, or computer network in one jurisdiction from another jurisdiction is deemed to have personally accessed the computer, computer system, or computer network in each jurisdiction." Cal. Pen. Code § 502.

246. Defendant violated Cal. Penal Code § 502(c)(2) by knowingly accessing and without permission taking, copying, analyzing, and using Plaintiff's and the California Subclass members' data.

247. Defendant effectively charged Plaintiff and the California Subclass members by taking, copying, analyzing, and using their valuable personal information without permission and exploiting that information for Defendant's own financial benefit.

248. Plaintiff and the California Subclass members retain a stake in the profits Defendant earned from their personal information and other data because, under the circumstances, it is unjust for Defendant to retain those profits.

249. As a direct and proximate result of Defendant's unlawful conduct within the meaning of Cal. Penal Code § 502, Defendant has caused loss to Plaintiff and the California Subclass members and has been unjustly enriched in an amount to be proven at trial.

250. Plaintiff, on behalf of himself and the California Subclass members, seek compensatory damages and/or disgorgement in an amount to be proven at trial, and declaratory, injunctive, or other equitable relief.

251. Plaintiff and the California Subclass members are entitled to punitive damages because Defendant's violations were willful and, upon information and belief, Defendant is guilty of oppression, fraud, or malice.

252. Plaintiff and the California Subclass members are also entitled to recover their reasonable attorneys' fees pursuant to Cal. Penal Code § 502(e).

EIGHTH CAUSE OF ACTION

CALIFORNIA'S UNFAIR COMPETITION LAW
Cal. Bus. & Prof. Code § 17200, *et seq.*
(On behalf of Plaintiff & the California Purchaser Subclass)

253. Plaintiff and the California Purchaser Subclass members incorporate the foregoing allegations as if fully set forth herein.

254. California's Unfair Competition Law ("UCL") prohibits any "unlawful, unfair, or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising." Cal. Bus. & Prof. Code § 17200.

255. Defendant's "unlawful" acts and practices include its violation of the Wiretap Act, 18 U.S.C. § 2510, *et seq.*; the California Invasion of Privacy Act, Cal. Penal Code §§ 631 and 632; the California Computer Data Access and Fraud Act, Cal. Penal Code § 502, *et seq.*; the DOJ Rule; Intrusion upon Seclusion, and Invasion of Privacy.

256. Defendant's conduct violated the spirit and letter of those laws, which protect property, economic and privacy interest and prohibits unauthorized disclosure of private communications and personal information.

257. Defendant's "unfair" acts and practices include its violation of property, economic and privacy interests protected by the statutes identified above.

258. To establish liability under the unfair prong, Plaintiff and California Purchaser Subclass members need not establish that these statutes were actually violated, although the claims pleaded herein do so.

259. Plaintiff and California Purchaser Subclass members have suffered injury-in-fact, including the loss of money and/or property as a result of Defendant's unfair and/or unlawful practices because they would not have used the Website or made purchases thereon, if they had known that their privacy would not be respected.

260. Defendant's actions caused damage to and loss of Plaintiff and the California Purchaser Subclass members because they would not have purchased from the Website if they had known that Defendant would not respect their privacy rights.

261. Defendant reaped unjust profits and revenue in violation of the UCL. This includes Defendant's profits and revenues from Plaintiff and California Purchaser Subclass members' personal information and communications. Plaintiff and the California Purchaser Subclass members seek restitution and disgorgement of these unjust profits and revenues.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Spencer Christy, individually and on behalf of all others similarly situated, respectfully requests that this Court enter judgment against Defendant Lenovo and in favor of Plaintiff and the Classes, and grant the following relief:

a. For an order certifying the Classes and naming Plaintiff as the representatives of the putative Classes and Plaintiff's attorneys as Class Counsel to represent the putative Class members;

b. For an order declaring that the Defendant's conduct violates the statutes and laws referenced herein;

c. For an order finding in favor of Plaintiff and the Classes on all counts asserted herein;

d. For statutory damages in amounts to be determined by the Court and/or jury;

e. For prejudgment interest on all amounts awarded;

f. For injunctive relief, restitution, and disgorgement, as pleaded or as the Court may deem proper; and

g. For an order awarding Plaintiff and the putative Classes their reasonable attorneys' fees and expenses and cost of suit.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury for all issues so triable.

Respectfully submitted,

Dated: February 5, 2026

By: */s/ Victor J. Sandoval*

Victor J. Sandoval, SBN 344461
ALMEIDA LAW GROUP LLC
111 W. Ocean Blvd Ste 426,
Long Beach, CA 90802
(562) 534-5907
victor@almeidalawgroup.com

David S. Almeida (*pro hac vice* forthcoming)
849 W. Webster Avenue
Chicago, Illinois 60614
(312) 576-3024
david@almeidalawgroup.com

Counsel for Plaintiff & the Proposed Classes