Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Assessing Health Data Privacy Damages During A Pandemic

By **Vildan Altuglu, Maria Salgado and Omur Celmanbet**

(September 8, 2020, 4:53 PM EDT)

Vildan Altuglu

Maria Salgado

Omur Celmanbet

The COVID-19 pandemic, which has generated a surge in telehealth and introduced the concept of contact tracing into our daily lives, is likely to expose businesses and governments to an increased risk of data privacy and data breach class actions related to health and other personal data.

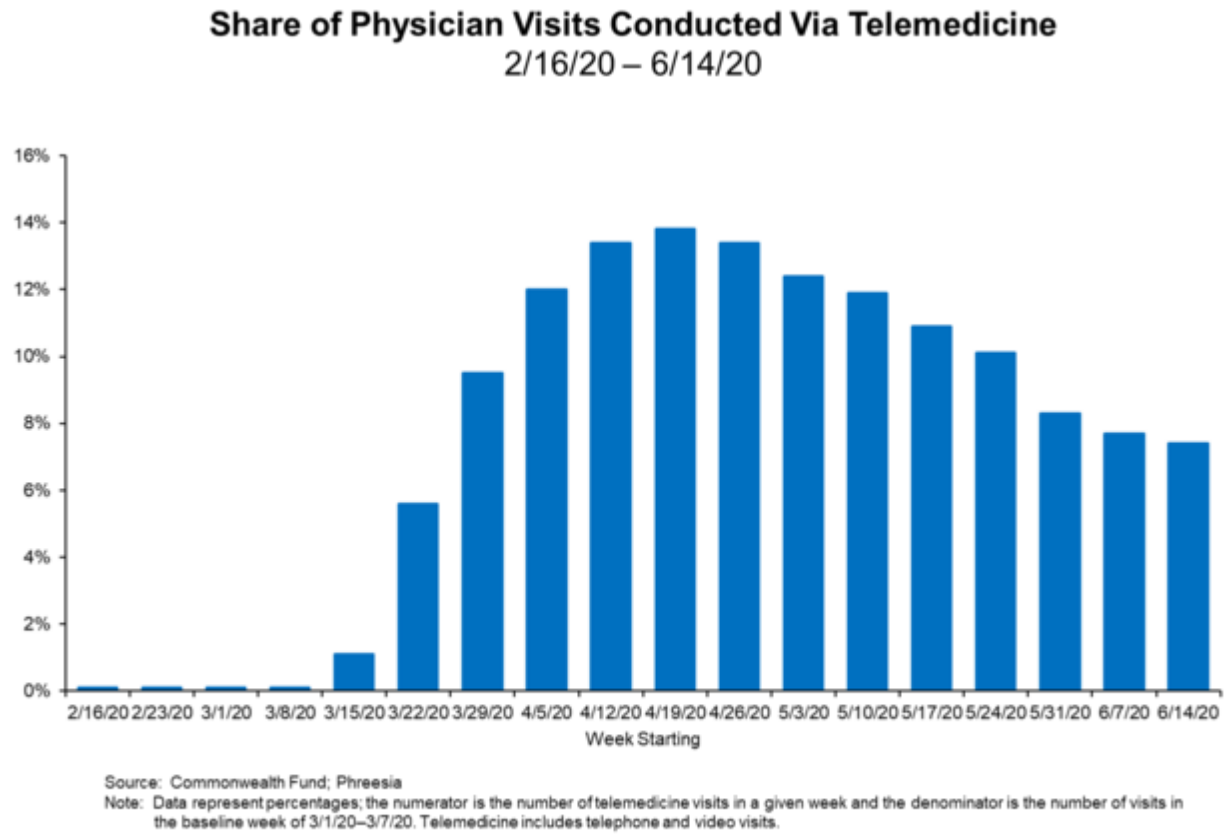
This article discusses potential economic approaches and challenges to valuing, in class action settings, alleged unconsented use or misappropriation of health and other private data generated during this health crisis.

Class Actions Related to Health Data Privacy and Data Breaches Are Expected to Rise During COVID-19

The spike in the use of telehealth has been one of the dramatic changes in health care delivery since the beginning of the COVID-19 pandemic. Telehealth includes, among others, the practice of doctors caring for patients remotely through the use of tools such as teleconferencing and videoconferencing.

The ability to receive care without having to travel to health care facilities has increased the appeal of telehealth, including telemedicine visits, for many patients during the pandemic. According to an April study, there is a strong correlation between the U.S. population's interest in telehealth and the number of COVID-19 cases.[1]

Similarly, an analysis published by the Commonwealth Fund shows that the share of physician visits conducted via telehealth was practically nonexistent in the first two months of 2020 and rose to nearly 14% by mid-April, as shown below.[2]



To facilitate the expansion of telehealth during the pandemic, in March the Office for Civil Rights at the U.S. Department of Health and Human Services lifted certain privacy and security compliance penalties and enforcement actions against providers, allowing them to use audio or video communication technologies, such as Facebook Messenger video chat, Google Hangouts video, Zoom and Skype, to provide remote health care services.[3]

Given the sensitive nature of the data exchanged during telehealth visits and stored by telehealth providers, the use of such communication technologies raises concerns about susceptibility of health and other personal data to unauthorized disclosures, uses, or misappropriation by unauthorized third parties, such as hackers.

These privacy and security concerns also extend to devices patients use to communicate and exchange data with their telehealth providers, including smartphones, tablets and computers as well as in-home patient monitors or other remote-care devices. Unauthorized third parties may obtain personal information, including health data and payment information, or infiltrate the larger networks of patient data in the event they are able to gain access to these connected devices.[4]

Contact tracing is another change facilitated by the pandemic that has led to an increase in exchange of personal data among individuals, companies and governments. Contact tracing is a public health management tool and involves identifying and monitoring individuals who had contact with infected individuals and notifying them of their potential exposure. While there is no compulsory digital COVID-19 contact tracing program in the U.S., multiple voluntary mobile apps developed by private companies exist.[5]

With contact tracing initiatives, the COVID-19 status and geolocation of individuals are collected, stored and also sometimes shared with various entities, raising data privacy and data breach concerns.[6] For example, geolocation data collected from smartphones with contact tracing apps may be used in isolation or in combination with other data to uncover a variety of information about individuals, including their routine activities (e.g., medical intake), interests (e.g., gym membership) and affiliations (e.g., religious affiliation).

Beyond concerns about public disclosure of this personal information, there are also concerns that hackers can create fake contact tracing apps, or send fake messages pretending to be contact tracers to initiate a malware attack or a phishing scam to extract credit card and other personal data.[7]

Accordingly, such changes instituted during the pandemic with regard to health care delivery and public health management are expected to increase class action litigation related to data privacy and data breaches in the health care industry.

Potential Economic Approaches and Challenges to Valuing Alleged Misuse or Misappropriation of Personal Data

Broadly, there are two types of consumer class actions related to personal data: (1) data privacy class actions where the data at issue was allegedly misused by the parties that received the data, and (2) data breach class actions where the data at issue was exposed and improperly accessed by unrelated third parties.

An example of the former is a federal lawsuit filed in 2018 against CVS Health Corp. due to its alleged exposure of the personal health information of over 6,000 individuals via clear-windowed mailings revealing their names, addresses and HIV status.[8] An example of the latter involves lawsuits against Anthem Inc. following a data breach incident that allegedly exposed personal data on 80 million individuals, including names, birth dates, medical identification numbers and social security numbers.[9]

In data privacy class actions, damages pursued are often based on alleged loss of intrinsic value of privacy and alleged unjust enrichment of the party that has misused the data. In data breach class actions, on the other hand, damages pursued are often based on actual fraud costs, future risk of identity theft and identity theft monitoring and prevention costs.[10] The economic approaches related to these theories of harm for telehealth, contact tracing and other personal data are discussed next.

Loss of Intrinsic Value of Privacy

This theory is traditionally built on the premise that keeping information private has a uniform economic value that is common to all individuals (e.g., a societal value), and unauthorized access to this information by a third party would result in the loss of that value.[11] Such a common, uniform value to privacy implies that the alleged injury is not specific to the individual or the infringing party, rendering an identical quantum of damages for each putative class member, regardless of their individual circumstances.

For example, under this theory, unauthorized use of geolocation or health data exchanged as part of COVID-19 contact tracing initiatives would generate the same amount of damages for each putative class member regardless of the extent of information provided by a given individual.

Similarly, unauthorized use of geolocation data accessed by means unrelated to the alleged misconduct

would generate identical damages (e.g., damages due to unauthorized use of geolocation data would be identical whether the data was accessed via a gaming app or via a contact tracing app).

Further, public disclosure of the at-issue information in other contexts (e.g., an infected individual posting COVID-19 status in a public Facebook profile) is unlikely to matter under the loss of intrinsic value of privacy theory.

Survey-based, quantitative approaches such as contingent valuation surveys and conjoint analysis have been proposed as suitable methods to estimate invasion of privacy damages in data privacy class actions.[12] In contingent valuation surveys, respondents are typically asked directly about their value for the conduct at issue.

In the data privacy context, this could include questions such as "how much would you pay to protect privacy of your data?" In conjoint analysis, respondents are typically asked to make choices from a small set of products and services in a series of survey questions.

In the data privacy context, each product or service shown to respondents (e.g., a new online video gaming service) would be described on the basis of the same set of features including a feature that relates to the use or sharing of personal data (e.g., type of game, number of players, whether the service shares players' personal data with advertisers) and a set of prices. Respondents' product choices that involve different feature combinations and prices are then used to estimate an average value for data privacy.

These approaches have been subject to a number of critiques.

First, both contingent valuation and conjoint analysis are stated preference methods in that they rely on what people say or imply they will do (i.e., based on their choices in a survey setting), and not on what they actually do.[13]

Second, in the privacy context, survey methods are subject to the so-called privacy paradox, the well-documented discrepancy between consumers' stated preferences for privacy and their privacy-related behaviors.[14]

Third, both methods have been shown to generate inflated values for privacy due to certain biases these surveys are susceptible to (e.g., conjoint surveys may artificially focus survey respondents on privacy).[15]

Further, reliably extrapolating the estimated average value of privacy beyond the survey samples (e.g., to the putative class as a whole) is challenging due to the extent of heterogeneity in consumers' privacy expectations and preferences.[16]

Unjust Enrichment

An alternative theory of harm put forward in data privacy class actions is based on the allegation that the infringing third party generated revenues and profits by using private data without authorization. Generating reliable estimates of privacy value based on this theory requires distinguishing and isolating the portion of the infringer's valuation, revenues or profits that is directly attributable to the alleged misuse of private data.

This can be a challenging exercise, as numerous factors may influence a firm's valuation, revenues, and profits. For example, determining the value to companies involved in an alleged unauthorized use of geolocation and other private data shared with contact tracing apps would require controlling for all factors that influence these companies' valuation, revenues and profits.

Actual Fraud Costs

In data breach class actions, one of the most commonly pursued type of damages involves actual fraud costs. In the case of breach of payment card data, for instance, this often involves determining fraudulent transactions and associated amounts on exposed accounts. However, because consumers typically share the same types of data with multiple parties and because concurrent data breach incidents have become increasingly common, it can be difficult to establish causality, or a nexus between fraudulent activity and a particular data breach incident.

According to a 2019 industry study, for example, there were 1,473 data breaches in the U.S. in 2019 alone, and over 164 million personally identifiable records were exposed in those breaches.[17] Similarly, a 2016 study showed that roughly 36 million U.S. adults received more than one notification of data breach between June 2014 and June 2015 alone.[18]

Risk of Future Identity Theft

Harm arising from the risk of future identity theft is also commonly pursued in data breach class actions. This theory of harm is based on the premise that the identity theft or other negative consequences of a data breach may not occur immediately. As such, it is argued that individuals whose information was breached should be compensated for the expected long-term impact of the data breach.

Historical evidence and academic literature, however, suggest that only a small number of individuals will experience any type of identity theft as a result of a data breach incident.[19] Moreover, it is difficult to predict who will be impacted: The probability that an individual will be subject to future identity theft can vary across individuals based on prior incidence of identity theft, number of companies that have access to the data at issue, and the type of data that was compromised.

Further, any methods proposed to calculate this type of damages would need to be able to isolate the incremental risk associated with the data breach for each individual in the future.

Identity Theft Monitoring and Prevention Costs

Yet another common type of damages asserted in data breach class actions is based on what consumers allegedly already paid or would likely pay for credit and identity theft monitoring and prevention services. These may include a range of services such as credit freezes with credit reporting agencies, identity theft insurance and credit monitoring services.

Since not everyone would sign up for these types of services, determining which members of a proposed class incurred or would likely incur such costs is central to quantifying these damages. Survey methods soliciting self-reported measures from a sample of putative class members on the costs already incurred and the probability of signing up for credit monitoring or identity theft insurance services may be used. The validity of these methods will in part depend on the reliability of the self-reported measures and on the representativeness of the survey respondents.

Additionally, real-world data may provide insight about the rate at which affected individuals are likely to sign up for credit and identity theft monitoring and prevention services. For example, many companies in the U.S. offer free credit monitoring services to individuals whose data were potentially exposed in a data breach incident. The share of individuals who sign up for these free services, which is typically low, can be informative of the share of individuals who would ultimately sign up and pay a fee for such services.

Vildan Altuglu and Maria Salgado are vice presidents and Omur Celmanbet is a principal at Cornerstone Research.

Cornerstone Research senior manager Rezwan Haque and associate Lucia Yanguas contributed to this article.

[1] Young-Rock Hong et al., "Population-Level Interest and Telehealth Capacity of US Hospitals in Response to COVID-19: Cross-Sectional Analysis of Google Search and National Hospital Survey Data,"JMIR Public Health and Surveillance6, no. 2 (2020): e18961.

[2] Ateev Mehrotra et al., "The Impact of the COVID-19 Pandemic on Outpatient Visits: A Rebound Emerges," The Commonwealth Fund, May 19, 2020.

[3] "Notification of Enforcement Discretion for Telehealth Remote Communications during the COVID-19 Nationwide Public Health Emergency," U.S. Department of Health and Human Services, available at https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html, last accessed March 27, 2020.

[4] See, e.g., Joseph L. Hall and Deven McGraw, "For Telehealth to Succeed, Privacy and Security Risks Must Be Identified and Addressed," Health Affairs 33, no. 2 (2014): 216–221. See also Lily Hay Newman, "Medical Devices Are the Next Security Nightmare," Wired, March 2, 2017.

[5] See "Coronavirus Disease 2019 (COVID-19): Contact Tracing," Centers of Disease Control and Prevention, August 4, 2020, available at https://www.cdc.gov/coronavirus/2019-ncov/daily-life-coping/contact-tracing.html.

[6] See Paige M. Boshell, "The Power of Place: Geolocation Tracking and Privacy," American Bar Association Business Law Section, March 25, 2019.

[7] See Stephen Silver, "Fake Contact Tracing Apps Could Install Malware on Your Smartphone," The National Interest, June 12, 2020. See also Lily Hay Newman, "Don't Be Fooled by Covid-19 Contact-Tracing Scams," Wired, May 25, 2020.

[8] Class Action Complaint, John Doe One et al. v. CVS Health Corp. et al., No. 2:18-cv-00238-EAS-CMV (S.D. Ohio, Mar. 21, 2018).

[9] Class Action Complaint, Brown v. Anthem Inc., No. 5:15-md-02617 (N.D. Cal., Feb. 13, 2015).

[10] See Vildan Altuglu, Lorin M. Hitt, S. Hussain, and M. Li Bergolis, "Valuation of Privacy: Assessing Potential Harm from Unauthorized Access and Misuse of Private Information in Consumer Class Actions," forthcoming in Legal Applications of Marketing Theory, eds. Professors Jacob Gersen and Joel Steckel.

[11] See Vildan Altuglu, Lorin M. Hitt, S. Hussain, and M. Li Bergolis, "Valuation of Privacy: Assessing Potential Harm from Unauthorized Access and Misuse of Private Information in Consumer Class Actions," forthcoming in Legal Applications of Marketing Theory, eds. Professors Jacob Gersen and Joel Steckel.

[12] See Vildan Altuglu, Lorin M. Hitt, S. Hussain, and M. Li Bergolis, "Valuation of Privacy: Assessing Potential Harm from Unauthorized Access and Misuse of Private Information in Consumer Class Actions," forthcoming in Legal Applications of Marketing Theory, eds. Professors Jacob Gersen and Joel Steckel.

[13] See, e.g., Jerry Hausman, "Contingent Valuation: From Dubious to Hopeless," Journal of Economic Perspectives 26, no. 4 (2012): 43–56.

[14] See, e.g., Sarah Spiekermann, Jens Grossklags, and Bettina Berendt, "E-Privacy in 2nd Generation E-commerce: Privacy Preferences versus Actual Behavior," in Proceedings of the 3rd ACM Conference on Electronic Commerce (2001): 38–47; Patricia A. Norberg, Daniel R. Horne, and David A. Horne, "The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors," Journal of Consumer Affairs 41, no. 1 (2007): 100–126; Idris Adjerid, Eyal Peer, and Alessandro Acquisti, "Beyond the Privacy Paradox: Objective Versus Relative Risk in Privacy Decision Making," MIS Quarterly 42, no. 2 (2018): 465–488; Alessandro Acquisti, Laura Brandimarte, and George Loewenstein, "Privacy and Human Behavior in the Age of Information," Science 347, no. 6221 (2015): 509–514 at 510.

[15] See, e.g., Jerry Hausman, "Contingent Valuation: From Dubious to Hopeless," Journal of Economic Perspectives 26, no. 4 (2012): 43–56.

[16] Academic research demonstrates that consumers differ in their privacy preferences and expectations and that consumers' privacy preferences and expectations can be context-dependent. See, e.g., Alessandro Acquisti, Laura Brandimarte, and George Loewenstein, "Privacy and Human Behavior in the Age of Information," Science 347, no. 6221 (2015): 509–514; Kirsten Martin and Katie Shilton, "Why Experience Matters to Privacy: How Context-Based Experience Moderates Consumer Privacy Expectations for Mobile Applications," Journal of the Association for Information Science and Technology67, no. 8 (2016): 1871–1882; Helen Nissenbaum, "Privacy as Contextual Integrity," Washington Law Review 79, no. 1 (2004): 119–157.

[17] "2019 End-Of-Year Data Breach Report," Identity Theft Resource Center, 2020, available at https://notified.idtheftcenter.org/s/resource.

[18] Lillian Ablon et al., "Consumer Attitudes toward Data Breach Notifications and Loss of Personal Information," Rand Corporation, 2016. The actual number of data breaches is likely to be higher: a recent study estimated the number of unreported data breaches may be equal to 25 percent to 85 percent of the number of reported breaches. See James T. Graves, Alessandro Acquisti, and Nicolas Christin, "Should Credit Card Issuers Reissue Cards in Response to a Data Breach? Uncertainty and Transparency in Metrics for Data Security Policymaking," ACM Transactions on Internet Technology

(TOIT) 18, no. 4 (2018): 1–19.1847, no. 6221 (2015): 509-514.

[19] See, e.g., "Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," U.S. Government Accountability Office, GAO-07-737, June 2007.