Alexander Shalom (BAR No. 021162004)
AMERICAN CIVIL LIBERTIES UNION
OF NEW JERSEY FOUNDATION
570 Broad Street, 11th Fl.
Post Office Box 32159
Newark, NJ 07102

SUPREME COURT OF NEW JERSEY

FACEBOOK, INC., *Plaintiff*, v. STATE OF NEW JERSEY *Defendant*.	: Criminal Action : No. 087054 : : Superior Court of New Jersey, : Appellate Division : Nos. A-3350-20, A-0119-21
IN THE MATTER OF THE APPLICATION OF THE STATE OF NEW JERSEY FOR A COMMUNICATIONS DATA WARRANT AUTHORIZING THE OBTAINING OF THE CONTENTS OF RECORDS FROM FACEBOOK, INC.	: Sat Below: : Hon. Jack M. Sabatino, P.J.A.D. : Hon. Garry S. Rothstadt, J.A.D. : Hon. Jessica R. Mayer, J.A.D.

BRIEF OF *AMICI CURIAE* AMERICAN CIVIL LIBERTIES UNION & AMERICAN CIVIL LIBERTIES UNION OF NEW JERSEY

Alexander Shalom (BAR No. 021162004)
Jeanne LoCicero (BAR No. 024052000)
AMERICAN CIVIL LIBERTIES UNION
OF NEW JERSEY FOUNDATION
570 Broad Street, 11th Fl.
Post Office Box 32159
Newark, NJ 07102
Tel: (973) 854-1714
ashalom@aclu-nj.org
jlocicero@aclu-nj.org

Jennifer Stisa Granick*
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
2101 Webster Street #1300
Oakland, CA 94612
Tel: (415) 343-0758
jgranick@aclu.org

* *Pro hac vice* pending

Attorneys for Amici Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES ii
PRELIMINARY STATEMENT 1
STATEMENT OF FACTS AND PROCEDURAL HISTORY 3
ARGUMENT 4
I. Today's data surveillance is far more invasive even than eavesdropping and wiretaps of old. 4
II. Under *Berger*, the Fourth Amendment requires that warrants seeking ongoing access to future private communications contain special safeguards, like those enshrined in Title III and the NJWESCA, regardless of whether acquisition is contemporaneous or not. 8
III. If the Court disagrees that the proposed series of ongoing acquisitions of electronic communications are an "interception", the *Berger* and subsequent electronic search cases nevertheless require strict adherence to Fourth Amendment safeguards. 13
IV. The New Jersey Constitution also requires these safeguards, as it is more protective than the federal Constitution. 19
CONCLUSION 22
APPENDIX OF *AMICI CURIAE* ..... Aai

TABLE OF AUTHORITIES

CASES

Anderson v. Maryland,
427 U.S. 463 (1976).....20

Berger v. New York,
388 U.S. 41 (1967)..... passim

California v. Greenwood,
486 U.S. 35 (1988).....26

Carpenter v. United States,
138 S. Ct. 2206 (2018) 11, 12, 19, 27

Facebook, Inc. v. State,
251 N.J. 378 (2022) 9

Facebook, Inc. v. State,
252 N.J. 36 (2022) 9

Facebook, Inc. v. State,
471 N.J. Super. 430 (App. Div. 2022) 8

Florida v. Bostick,
501 U.S. 429 (1991).....26

Heien v. North Carolina,
574 U.S. 54 (2014).....26

In re [REDACTED]@gmail.com,
62 F. Supp. 3d 1100 (N.D. Cal. 2014) 22

In re Grand Jury Subpoena,
828 F.3d 1083 (9th Cir. 2016) 12

In re Search of Google Email Accounts identified in Attachment A,
92 F. Supp. 3d 944 (D. Alaska 2015).....22

In re Search of Info. Associated With Four Redacted Gmail Accounts,
371 F. Supp. 3d 843 (D. Or. 2018).....23

In re Three Hotmail Email Accounts,
No. 16-MJ-8036-DJW, 2016 WL 1239916 (D. Kan. Mar. 28, 2016) 21

Osborn v. United States,
385 U.S. 323 (1966).....15

Rakas v. Illinois,
439 U.S. 128 (1978).....25

Richardson v. State,
No. 46, 2022 WL 3711713 (Md. August 29, 2022).....21

Riley v. California,
573 U.S. 373 (2014)..... 11, 12, 20

Schneckloth v. Bustamonte,
412 U.S. 218 (1973).....26

Smith v. Maryland,
442 U.S. 735 (1979).....27

State v. Alston,
88 N.J. 211 (1981) 25

State v. Ates,
217 N.J. 253 (2014) 24

State v. Carter,
247 N.J. 488 (2021) 25

State v. Carty,
170 N.J. 632 (2002) 26

State v. Cooke,
163 N.J. 657 (2000) 25

State v. Domicz,
188 N.J. 285 (2006) 26

State v. Earls,
214 N.J. 564 (2013) 27

State v. Fairley,
457 P.3d 1150 (Wash. Ct. App. 2020) 21

State v. Feliciano,
224 N.J. 351 (2016) 24

State v. Hempele,
120 N.J. 182 (1990) 25, 26

State v. Johnson,
68 N.J. 349, 353–54 (1975).....26

State v. McAllister,
184 N.J. 17 (2005) 26

State v. Novembrino,
105 N.J. 95 (1987) 25

State v. Reid,
194 N.J. 386 (2008) 27

State v. Smith,
278 A.3d 481 (Conn. 2022).....21

United States v. Abboud,
438 F.3d 554 (6th Cir. 2006).....22

United States v. Christie,
624 F.3d 558 (3d Cir. 2010).....27

United States v. Comprehensive Drug Testing, Inc.,
621 F.3d 1162 (9th Cir. 2010) 11, 24

United States v. Diaz,
841 F.2d 1 (1st Cir. 1988) 22

United States v. Espudo,
954 F. Supp. 2d 1029 (S.D. Cal. 2013).....16

United States v. Griffith,
867 F.3d 1265 (D.C. Cir. 2017).....23

United States v. Leon,
468 U.S. 897 (1984).....25

United States v. Miller,
425 U.S. 435 (1976).....26

United States v. Shipp,
392 F. Supp. 3d 300 (E.D.N.Y. 2019)..... 12, 21

United States v. Warshak,
631 F.3d 266 (6th Cir. 2010).....12

United States v. Wey,
256 F. Supp. 3d 355 (S.D.N.Y. 2017)..... 21, 22

STATUTES

New Jersey Wiretapping and Electronic Surveillance Act, ... 7, 8, 18

N.J.S.A. 2A:156A-12 7

N.J.S.A. 2A:156A-1–26 25

N.J.S.A. 2A:156A-2 7

Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. 90-351, Title III, 18 U.S.C. §§ 2510–20 ..... 7, 8, 18

OTHER AUTHORITIES

Antonio Regalado, *Who Coined 'Cloud Computing'?*, MIT Tech. Rev. (Oct. 31, 2011) 9

Apple, *iCloud Storage Plans and Pricing* 10

Dropbox, *Choose the Right Dropbox for You* 10

Dropbox, *How Much is 1 TB of Storage?* 10

Google One, *One Membership to Get More Out of Google* 10

Microsoft 365, *OneDrive PC folder backup* 10

Microsoft, *OneDrive Personal Cloud Storage* 10

Samuel Gibbs, *How Did Email Grow from Messages Between Academics to a Global Epidemic?*, Guardian (Mar. 7, 2016) 9

PRELIMINARY STATEMENT

The Appellate Division concluded that so long as the State makes a single showing of probable cause, the sole limitation on the State's ability to surveil an individual's prospective private communications is Rule 3:5-5(a), which requires that a warrant be executed within 10 days of issuance. Under the ruling below, therefore, courts can issue warrants for communications and related data (communications data warrants or "CDWs") so long as the surveillance is limited to 10 days' worth of future conversations. This ongoing communications surveillance, the Appellate Division held, is not subject to enhanced safeguards contained in Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510 *et seq*. (hereinafter "Wiretapping and Electronic Surveillance Act" or "Title III")[1], or the equivalent provisions of the New Jersey Wiretapping and Electronic Surveillance Act ("NJWESCA"), N.J.S.A. 2A:156A-2, 2A:156A-12.

The Appellate Division's conclusion is wrong, and Meta's argument that a CDW cannot authorize ongoing surveillance of future communications is correct. The Appellate Division's ruling violates *Berger v. New York*, 388 U.S. 41 (1967), with deeply troubling consequences for privacy in modern digital

[1] Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. 90-351, Title III, 18 U.S.C. §§ 2510–20.

communications. In *Berger*, the U.S. Supreme Court held that the sensitivity of and privacy interest in private conversations require enhanced procedural safeguards to cabin executive discretion, minimize the risk of abuse, and avoid the problem of general warrants. *Id.* In response to *Berger*, the U.S. Congress and state legislatures, including New Jersey's, passed comprehensive legislation regulating wiretaps and electronic surveillance. *See* Wiretapping and Electronic Surveillance Act; NJWESCA. These statutes govern prospective, ongoing searches and seizures of communications, and the surveillance at issue here can only be constitutionally conducted with the kinds of safeguards that these statutes provide.

Indeed, regardless of whether the novel surveillance here is labeled an "interception," the constitutional concerns that motivated the *Berger* Court plainly apply and should guide this Court's ruling. In the five decades since *Berger*, technological developments have vastly expanded the universe of private communications susceptible to government intrusions and at risk of indiscriminate government rummaging. Service providers now store extensive records of past conversations, far more revealing even than the eavesdropping or wiretapping of old. In 1967, police had to tap into conversations at the right place and the right time, or the conversations instantly disappeared. Now, law enforcement can go back in time, and scour vast repositories of emails, texts,

direct messages, photos, location data, search histories, and more. As with the interception of current or prospective conversations, when law enforcement engages in surveillance of sensitive digital communications content, the Constitution requires scrupulous adherence to the dictates of the Fourth Amendment, especially the particularity requirement, to balance the relationship between the state and the individual and to ensure that police do not abuse the extensive access modern technology affords to intimate matters.

Finally, the New Jersey Constitution provides protections beyond those of the Fourth Amendment, and therefore dictates that this Court hold that the types of protections codified in Title III and the NJWESCA must also apply to the communications surveillance at issue here.

STATEMENT OF FACTS AND PROCEDURAL HISTORY

For the purpose of this brief, *amici* accept the statement of facts and procedural history contained in Meta's Appellate Division brief, adding the following: The Appellate Division affirmed the trial court's quashing of the communication data warrants, but held that wiretap orders were not required. *Facebook, Inc. v. State*, 471 N.J. Super. 430, 436 (App. Div. 2022). The panel imposed certain temporal limitations on the use of communication data warrants. *Id.* Thereafter, Facebook sought leave to appeal, which this Court

granted. *Facebook, Inc. v. State*, 251 N.J. 378 (2022). The State sought and obtained leave to cross-appeal. *Facebook, Inc. v. State*, 252 N.J. 36 (2022).

ARGUMENT

I. Today's data surveillance is far more invasive even than eavesdropping and wiretaps of old.

Computers and other digital devices contain an immense amount of private, sensitive data. Three and a half decades separate the world's first e-mail message[2] from the vast storage and communicative capacities of cloud computing.[3] With cloud computing, previously unimaginable troves of information—including private photos, voice recordings, videos, documents, diaries, correspondence, appointments, medical records, and more—are stored by third-party companies and can be accessed by a user at any time, via any device with an Internet connection.

These advances also mean that individuals can engage in an increasing variety and volume of cloud-based electronic communications, including emails, SMS and text messages, chats on messaging apps, and social media messages. Those communications can include not just conversations, but also

---

[2] Samuel Gibbs, *How Did Email Grow from Messages Between Academics to a Global Epidemic?*, Guardian (Mar. 7, 2016) (Aa29).

[3] Antonio Regalado, *Who Coined 'Cloud Computing'?*, MIT Tech. Rev. (Oct. 31, 2011) (Aa2) (noting 2006 as the year Google's Eric Schmidt introduced the term to an industry conference, with the term quickly gaining popularity after).

all of the kinds of digital files now stored in our devices and on our Internet accounts.

In recent years, the use of cloud-based services for digital storage and communication has skyrocketed. Today's most popular cloud storage platforms allow personal users to store massive quantities of personal information on their servers. Microsoft, Dropbox, Apple, and Google all offer their users several gigabytes of data storage for free and up to two terabytes by subscription.[4] A terabyte of cloud storage totals over 250,000 personal photos, nearly 21 continuous days of high-definition video, or the equivalent of 6.5 million pages of documents spanning 1,300 physical filing cabinets.[5]

With many cloud-based services, users can set up their systems so that their personal data and files are instantaneously and automatically transmitted from their local computer or hard drive, and stored on remote servers.[6] The owner can then access those files, share access with others, and maintain control across platforms over who has editing access or viewing rights. The low cost of cloud storage also means that social media companies allow users

---

[4] Microsoft, *OneDrive Personal Cloud Storage* (Aa25); Dropbox, *Choose the Right Dropbox for You* (Aa12); Apple, *iCloud Storage Plans and Pricing* (Aa8); Google One, *One Membership to Get More Out of Google* (Aai).

[5] Dropbox, *How Much is 1 TB of Storage?* (Aa17).

[6] Microsoft 365, *OneDrive PC folder backup* (Aa20).

to constantly add content—conversations, photos, videos, audio recordings, and other files—without having to delete older data, resulting in years of personal and communicative information stored online.

In short, today's digital platforms store far more information revealing individuals' private matters than one could obtain from past physical analogs. *See Riley v. California*, 573 U.S. 373, 394–95 (2014); *see also United States v. Comprehensive Drug Testing, Inc.* (hereinafter "*CDT*"), 621 F.3d 1162, 1175 (9th Cir. 2010) (en banc) (per curiam).

Because online accounts "collect[ ] in one place many distinct types of information"—for example, an address, a note, a prescription, a bank statement, or a video—digital data "reveal much more in combination than any isolated record," *Riley*, 573 U.S. at 394, and they reveal much more about "an individual's private interests or concerns." *Id.* at 395. Moreover, while our garages and desk drawers may fill all the way up with knickknacks, requiring periodic spring cleaning, digital data can pile up and persist indefinitely. Law enforcement access to electronically stored data can expose years'—even decades'—worth of personal information. *See Carpenter v. United States*, 138 S. Ct. 2206, 2218 (2018); *Riley*, 573 U.S. at 394. This combination of volume, depth, and longevity of personal information raises severe privacy risks when it comes to digital searches.

Technology has also given law enforcement the ability to obtain previously unknowable information, *Carpenter*, 138 S. Ct. at 2217–18, such as records of what we read (Internet browsing history), where we've gone (location history), what we've said (extensive conversations in the form of email or text), and to whom we've said it (associational information), along with efficient and centralized access to medical records and other sensitive information. Courts have already recognized some of these categories of information as deserving of particularly stringent privacy protections. *See, e.g.*, *Riley*, 573 U.S. at 395–96 (search and browsing history "could reveal an individual's private interests or concerns—perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD") ; *United States v. Warshak*, 631 F.3d 266, 286 (6th Cir. 2010) (email); *In re Grand Jury Subpoena*, 828 F.3d 1083 (9th Cir. 2016) (same). As the Ninth Circuit has explained, "searches of computers therefore often involve a degree of intrusiveness much greater in quantity, if not different in kind, from searches of other containers." *United States v. Payton*, 573 F.3d 859, 862 (9th Cir. 2009).[7]

[7] In addition, searches of computers or other digital devices that are connected to the Internet present risks that law enforcement searching through a device could access more than locally stored physical media but online accounts, too. *See, e.g.*, *United States v. Shipp*, 392 F. Supp. 3d 300, 308 (E.D.N.Y. 2019) (Police access to social media accounts and online communications services

II. Under *Berger*, the Fourth Amendment requires that warrants seeking ongoing access to future private communications contain special safeguards, like those enshrined in Title III and the NJWESCA, regardless of whether acquisition is contemporaneous or not.

The Supreme Court's decision in *Berger* governs the ongoing surveillance of future private communications at issue in this case. The State asserts that it may obtain multiple disclosures of future private electronic communications without complying with either the federal or state wiretap and electronic surveillance statutes, solely because the technological means of transmitting information over the Internet involves temporary storage on a provider's servers. However, the State cannot avoid the constitutional safeguards that *Berger* prescribes by pointing to minor technological differences between how companies facilitated prospective communications surveillance in the 1960s and today.

In *New York v. Berger*, the U.S. Supreme Court held that a New York statute—which authorized the interception of communications based only on reasonable grounds to believe that evidence of crime may be obtained—violated the Fourth Amendment. 388 U.S. 41 (1967). The New York statute

---

present a "threat [that] is further elevated . . . because, perhaps more than any other location—including a residence, a computer hard drive, or a car—[they] provide[] a single window through which almost every detail of a person's life is visible.").

did not require particularity as to the communications, conversations, or discussions to be seized, the facilities where the interception would take place, or the communications that would be obtained. Nor did it require a showing of necessity, minimization of innocent or irrelevant conversations, nor reporting to the judge. *Id.* at 59.

In ruling the New York statute unconstitutional, the Court noted that access to "private discourse" is particularly invasive and susceptible to abuse. *Id.* at 45. Indeed, eavesdropping invades "the innermost secrets of one's home or office," *id.* at 63, and presents "inherent dangers." *Id.* at 60. Eavesdropping "involve[d] an intrusion on privacy that is broad in scope," *id.* at 56.

In particular, the Court held that the New York statute violated the Fourth Amendment in part because it permitted a single warrant to authorize multiple prospective searches and seizures. The Court stated that eavesdropping for a two-month period was "[the] equivalent of a series of intrusions, searches and seizures pursuant to a single showing of probable cause[,] . . . [and avoids] prompt execution." *Id.* at 59. The Fourth Amendment requires that continuation of surveillance be based on "*present* probable cause," and not on the probable cause showing in the original warrant. *Id.* Yet that is exactly what the State seeks to do here.

The Court further noted that the search was unreasonable because of its impact on uninvolved third parties. "During such a long and continuous (24 hours a day) period[,] the conversations of any and all persons coming into the area covered by the device will be seized indiscriminately and without regard to their connection with the crime under investigation." *Id.* Again, the information the State would obtain should this warrant be enforced will have a broad impact over a much longer period of time than a day.

To illustrate the lack of adequate protections in the New York law, the Court compared warrants authorized by the New York statute to a court order it upheld in another case, *Osborn v. United States*, 385 U.S. 323 (1966). In particular, the Court noted that the *Osborn* warrant "authorized *one limited intrusion*[,] *rather than a series or a continuous surveillance*." 388 U.S. at 57 (emphasis added). The Court also noted that the *Osborn* officer's subsequent searches were based on a new probable cause order. Further, the officer executed the warrants "with dispatch, and not over a prolonged and extended period." *Id.* In contrast, the State here seeks an order permitting a series of intrusions, based on one showing of probable cause, and without need to go back to court to resume or initiate a new search. The surveillance would take place over a prolonged period. Such an order would violate the Fourth Amendment for the same reason that the statute in *Berger* did. *Id*.

The State argues that it need not comply with the dictates of *Berger*, and thus not of the federal or state statutes that apply to wiretaps and electronic surveillance, because it has contrived to avoid an "interception," which, it says, means only the acquisition of the contents of communications *contemporaneous* with their transmission. The State's legal argument exploits the "store and forward" nature of the computer protocols underlying the Internet, even though the information it seeks to obtain is functionally indistinguishable from what a wiretap would produce, but without the constitutionally-required safeguards. *Cf. United States v. Espudo*, 954 F. Supp. 2d 1029, 1034–35 (S.D. Cal. 2013) (holding that when the government "obtain[s] cell site location data for forward-looking periods of time," it must abide by the rules governing real-time surveillance, notwithstanding that the data is "maintained by the cell phone provider, however briefly, before it [is] sent to the Government").

Moreover, *Berger* does not draw the sharp line between contemporaneous and stored communications that the State says it does. While *Berger* uses the term "intercept," it does not define it as "contemporaneous acquisition." To the extent the examples in *Berger* involved contemporaneous access, that is likely because, in 1967, such access was the only reliable way to obtain private conversations. Then, as people talked, the words disappeared

forever unless someone was right there to hear them or had devised physical means to record them.

But nothing in *Berger*'s reasoning turns on whether the intrusions are contemporaneous or delayed by 15 minutes. The *Berger* Court's analysis was based on the invasiveness of government access to private conversations, and not the technology by which police accomplish the surveillance. While legislatures subsequently sought to implement the constitutionally-required safeguards in statutes regulating "wiretaps and electronic surveillance," *see* Wiretapping and Electronic Surveillance Act *and* NJWESCA, *Berger* itself emphasized how its principles reached a variety of surveillance methods. Indeed, the Court noted how communications surveillance had evolved through the years, from eavesdroppers lurking near windows or walls to intercepting telegraph signals, connecting to a telephone line, planting "bugs," beaming electronic rays at walls or glass windows, using tiny concealed or parabolic microphones, or employing a combination mirror transmitter that transmits images as well as sounds. 388 U.S. at 45–47. It explained that "few threats to liberty exist which are greater than that posed by the use of eavesdropping devices," regardless of the nature of that device. *Id.* at 63.

Berger is clear that law enforcement access to ongoing private electronic communications requires safeguards beyond a traditional warrant. The State

would use a technological wrinkle to gain exactly that kind of broad access on a repeated, prospective basis, with just one probable cause showing and without showing necessity, minimization, or particularity as to conversations or facilities, and without following other procedures acclaimed in *Berger* and codified in statute. But *Berger*'s reasoning does not depend on the technology employed. The *Berger* safeguards enshrined in New Jersey's wiretapping statute apply to conversation surveillance accomplished by ongoing access to today's online accounts, just as much as they do to surveillance accomplished by ongoing access to private communications using older techniques such as telephone surveillance. For these reasons, Meta's view that a CDW is insufficient and the State must comply with Title III and the NJWESCA is correct.

III. If the Court disagrees that the proposed series of ongoing acquisitions of electronic communications are an "interception", the *Berger* and subsequent electronic search cases nevertheless require strict adherence to Fourth Amendment safeguards.

Surveillance that by its nature involves a broad intrusion on conversational privacy requires strict adherence to the Fourth Amendment's requirements. In light of the extraordinary volume and breadth of sensitive information contained in today's electronically stored and transmitted information, warrants must impose clear limitations on law enforcement's electronic searches and seizures so as to avoid unnecessary exposure of our

intimate details to investigators. Even if the Court disagrees that the wiretapping statutes apply to this case, it should nevertheless ensure that the CDWs here specify the category of data, date range, or other fact-specific criteria that will ensure particularity and guard against overbreadth, and not authorize a "printout of everything that the user has". *State's Br. in Opp'n to FB's Mot. to Appeal*, at 2. In addition, courts can and sometimes must require investigators to report back, to segregate non-responsive data through the use of clean teams or other means, to delete irrelevant data, and to comply with other privacy-protecting practices to ensure that searches are constitutional.

The Fourth Amendment is intended "to place obstacles in the way of a too permeating police surveillance." *Carpenter*, 138 S. Ct. at 2214 (citation and quotation marks omitted). It requires that search warrants particularly describe the places to be searched and the things to be seized (particularity), and prohibits search for or seizure of anything for which there is not probable cause (overbreadth). Even in the context of warrants authorizing the search and seizure of a person's physical papers, the Supreme Court has long recognized the grave dangers of government access to papers without probable cause. As a result, "responsible officials, including judicial officials, must take care to assure that [searches and seizures] are conducted in a manner that minimizes unwarranted intrusions upon privacy." *Anderson v. Maryland*, 427 U.S. 463,

482 n.11 (1976). These concerns are especially salient in the face of expanding technological search capabilities, *see Riley*, 573 U.S. at 394–95, and *Berger*'s warnings about the "inherent dangers" of unbounded electronic searches and seizures hold true whether law enforcement seeks to obtain future communications or a complete record of those that have already occurred. 388 U.S. at 58–60.

Critically for the account searches and seizures at issue here, the Fourth Amendment requires that searches and seizures be limited by time frame, to relevant categories of information, and by other case-specific factors to the extent possible. There is no need for—and the Fourth Amendment does not allow—"all-content" CDWs demanding seizure of any account content or digital files that might exist.

First, courts regularly require the government to specify discrete categories of digital information to satisfy particularity and obtain a valid warrant. For example, in one federal investigation of an illegal firearms charge, a search warrant demanded that Facebook provide all the user's personal information, activity logs, photos, videos, posts, private messages, chats, friend requests, video call history, check-ins, IP logs, "likes," use of Facebook Marketplace, payment information, privacy settings, blocked users, tech support requests, and more. *United States v. Shipp*, 392 F. Supp. 3d 300,

303–06 (E.D.N.Y. 2019). In another, the government sought all financial records, notes, memoranda, records of internal and external communications, correspondence, audio tapes, video tapes, and photographs, among other information. *United States v. Wey*, 256 F. Supp. 3d 355, 364–66 (S.D.N.Y. 2017). Both courts held that warrants for seizure of any category of data without "link[ing] the evidence sought to the criminal activity supported by probable cause" did "not satisfy the particularity requirement." *Id.* at 387 (citatons omitted); *Shipp*, 392 F. Supp. 3d at 307. *See also In re Three Hotmail Email Accounts*, No. 16-MJ-8036-DJW, 2016 WL 1239916 (D. Kan. Mar. 28, 2016), *overruled in part by In re Info. Associated With Email Addresses Stored at Premises Controlled by the Microsoft Corp.*, 212 F. Supp. 3d 1023 (D. Kan. 2016) (denying warrant to search all content of email accounts).

State courts agree with this principle in the context of both social media and cell phone searches and seizures. *See Richardson v. State*, No. 46, 2022 WL 3711713 (Md. August 29, 2022) ("all-content" warrant to search cell phone should have been limited by time frame and categories of data); *State v. Smith*, 278 A.3d 481 (Conn. 2022) (warrant did not sufficiently limit the search of the contents of a cell phone by a description of the areas within the phone to be searched or by a time frame reasonably related to the crimes); *State v. Fairley*, 457 P.3d 1150 (Wash. Ct. App. 2020) (Fourth Amendment's

particularity requirement is of heightened importance when searching repositories for expressive materials, in the context of cell phones). Thus, courts should authorize seizure of only those categories of data likely to contain evidence of the crime. Without that limitation, a search is overbroad.

Second, seizures of account data should be limited by timeframe. CDWs can easily accomplish this. If an offense allegedly took place in 2021, police should not need obtain email from any other year, never mind a copy of the entire account, as it appears the State is seeking here. *See United States v. Abboud*, 438 F.3d 554, 576 (6th Cir. 2006) ("Failure to limit broad descriptive terms by relevant dates, when such dates are available to the police, will render a warrant overbroad." (citations omitted)); *United States v. Diaz*, 841 F.2d 1, 4–5 (1st Cir. 1988) (warrant overbroad when authorized seizure records before the first instance of wrongdoing mentioned in the affidavit); *In re [REDACTED]@gmail.com*, 62 F. Supp. 3d 1100, 1104 (N.D. Cal. 2014) (no warrant issued where government did not include a date limitation); *In re Search of Google Email Accounts identified in Attachment A*, 92 F. Supp. 3d 944 (D. Alaska 2015) (application without date restriction denied as overbroad).

Third, when available, courts can and should also use other criteria of digital information to constrain police and ensure that seizures are scoped to

probable cause, and that the warrant particularly describes the proper data to search, and what to search for. *See United States v. Griffith*, 867 F.3d 1265, 1276 (D.C. Cir. 2017) (deeming a warrant's failure to narrow a search based on ownership of a cell phone to be insufficiently particular). For example, if conversations between the target and known co-conspirator are potential evidence of a crime, the warrant could demand that Facebook turn over only messages between those two people. *In re Search of Info. Associated With Four Redacted Gmail Accounts*, 371 F. Supp. 3d 843, 845 (D. Or. 2018) (warrant for all emails associated with suspect's account is overbroad because Google is able to disclose only those emails the government has probable cause to search). If investigators' analysis reveals that another person may be involved, law enforcement can get a warrant to expand the search. But, as *Berger* points out, "conversations of any and all persons" should not be "seized indiscriminately and without regard to their connection with the crime under investigation." 388 U.S. at 59. Yet, that is what a "snapshot" of a Facebook account does.

Finally, depending on the facts of the investigation, which judges have access to via affidavits in support of warrants, courts may further constrain potentially abusive rummaging through private data. To protect the intermingled information that investigators do not have probable cause to seize

or review, courts can enhance oversight by imposing search protocols or requiring forensic examiners to log queries for later judicial review. Courts might also require law enforcement to use clean teams, and to segregate and delete irrelevant data, or implement other privacy-protecting means as may be appropriate. *CDT*, 621 F.3d at 1177.

In sum, the surveillance here must be conducted under the safeguards prescribed in *Berger* and implemented by Title III and the NJWESCA. *See* Part II *supra*. But if the Court disagrees, a CDW for one or more complete "snapshots" of a Facebook account should only issue if it closely adheres to Fourth Amendment safeguards. Failure to do so can put the target and everyone he or she communicates with at risk of a series of general searches and seizures that could be easily abused.

IV. The New Jersey Constitution also requires these safeguards, as it is more protective than the federal Constitution.

Although New Jersey's Wiretap and Electronic Surveillance Act, NJWESCA, N.J.S.A. 2A:156A-1–26, was modeled after Title III of the Omnibus Crime and Safe Streets Act, 18 U.S.C. §§ 2510–20, *State v. Ates*, 217 N.J. 253, 266 (2014), courts interpreting the state law must look to the State Constitution to ensure their interpretation "safeguard[s] an individual's right to privacy." *State v. Feliciano*, 224 N.J. 351, 370, 372–77 (2016) (*quoting Ates*, 217 N.J. at 268). The United States Constitution, as interpreted by the United

States Supreme Court, provides important guidance for this Court. But as the Court has emphasized before, while those interpretations "may serve to guide us in our resolution of New Jersey issues, 'we bear ultimate responsibility for the safe passage of our ship.'" *State v. Cooke*, 163 N.J. 657, 666–67 (2000) (quoting *State v. Hempele*, 120 N.J. 182, 196 (1990)). For more than four decades the New Jersey Constitution has protected individuals' rights where its federal counterpart has not. *See State v. Alston*, 88 N.J. 211, 225 (1981) (discussing divergence from federal constitutional jurisprudence).

New Jersey courts recognize that the State Constitution provides greater protections than its federal counterpart in a host of relevant contexts. For example, New Jersey courts have refused to erect barriers to civilians' ability to challenge unlawful searches and seizures. *Compare Alston*, 88 N.J. at 228–29 (taking broad view of standing to challenge validity of searches), *with Rakas v. Illinois*, 439 U.S. 128, 134 (1978) (taking narrow view). When a police officer violates a person's rights, the New Jersey Constitution provides a remedy, regardless of the officer's subjective intent. *Compare State v. Novembrino*, 105 N.J. 95, 157–58 (1987) (rejecting good-faith exception to the exclusionary rule) *and State v. Carter*, 247 N.J. 488, 532 (2021) (declining, under the State Constitution, to adopt a reasonable mistake of law exception) *with United States v. Leon*, 468 U.S. 897, 905 (1984) (recognizing good-faith

exception) *and Heien v. North Carolina*, 574 U.S. 54, 61 (2014) (finding stop justified even when based on a reasonable mistake about what the law forbids). Similarly, New Jersey Courts have recognized the peril of allowing police to easily circumvent the warrant requirement through a lax view of consent. *Compare State v. Johnson*, 68 N.J. 349, 353–54 (1975) (requiring showing that consent to search was knowingly given) *and State v. Carty*, 170 N.J. 632, 651 (2002) (disallowing routine requests for consent to search in automobile stops) *with Schneckloth v. Bustamonte*, 412 U.S. 218, 225 (1973) (requiring simply that consent to search be voluntary) *and Florida v. Bostick*, 501 U.S. 429, 434 (1991) (approving routine requests for consent without reasonable suspicion).

Most critically here, this Court has found expectations of privacy where the United States Supreme Court and some federal appellate courts have not, recognizing the vast swaths of personal information that would be revealed in a search of curbside garbage (*compare Hempele*, 120 N.J. at 215 (expectation of privacy in curbside trash) *with California v. Greenwood*, 486 U.S. 35, 37 (1988)), bank records (*compare State v. McAllister*, 184 N.J. 17, 26 (2005) (expectation of privacy in bank records) *with United States v. Miller*, 425 U.S. 435, 442 (1976) (no expectation of privacy in bank records)), utility records (*compare State v. Domicz*, 188 N.J. 285, 299 (2006) (acknowledging expectation of privacy in utility records) *with Smith v. Maryland*, 442 U.S.

735, 743–44 (1979) (no expectation of privacy in calling records)), Internet Service Provider subscription records (*compare State v. Reid*, 194 N.J. 386, 389 (2008) (expectation of privacy in Internet Service Provider records) *with, e.g.*, *United States v. Christie*, 624 F.3d 558, 574 (3d Cir. 2010) (no expectation of privacy in Internet Service Provider records)), and cellphone location (*compare State v. Earls*, 214 N.J. 564, 585 (2013) (expectation of privacy in real-time cell phone location data) *with Carpenter*, 138 S. Ct. at 2220 (finding expectation of privacy in historical cell phone location data, but expressing no view on real-time cell tracking)).

As discussed above, the United States Constitution requires at least as much restraint and as many safeguards as a wiretap order for the prospective surveillance the State is asking for here. The New Jersey Constitution requires at least as much as well, if not more.

CONCLUSION

For the reasons set forth above, the Court should hold that the privacy protections codified in Title III and the NJWESCA apply to the communications surveillance at issue here.

Dated: October 5, 2022

Respectfully submitted,

Alexander Shalom (BAR No. 021162004)
Jeanne LoCicero (BAR No. 024052000)
AMERICAN CIVIL LIBERTIES UNION
OF NEW JERSEY FOUNDATION
570 Broad Street, 11th Fl.
Post Office Box 32159
Newark, NJ 07102
Tel: (973) 854-1714
ashalom@aclu-nj.org
jlocicero@aclu-nj.org

Jennifer Stisa Granick*
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
2101 Webster Street #1300
Oakland, CA 94612
Tel: (415) 343-0758
jgranick@aclu.org

* *Pro hac vice* pending

Attorneys for Amici Curiae

APPENDIX OF *AMICI CURIAE* AMERICAN CIVIL LIBERTIES UNION & AMERICAN CIVIL LIBERTIES UNION OF NEW JERSEY

TABLE OF APPENDIX CONTENTS

Google One, *One Membership to Get More Out of Google*, https://one.google.com/about ..... Aai

Antonio Regalado, *Who Coined 'Cloud Computing'?*, MIT Tech. Rev. (Oct. 31, 2011) Aa1

Apple, *iCloud Storage Plans and Pricing* Aa7

Dropbox, *Choose the Right Dropbox for You* Aa11

Dropbox, *How Much is 1 TB of Storage?* Aa16

Microsoft 365, *OneDrive PC folder backup* Aa19

Microsoft, *OneDrive Personal Cloud Storage* Aa24

Samuel Gibbs, How Did Email Grow from Messages Between Academics to a Global Epidemic?, Guardian (Mar. 7, 2016) Aa28

MIT Technology Review Subscribe

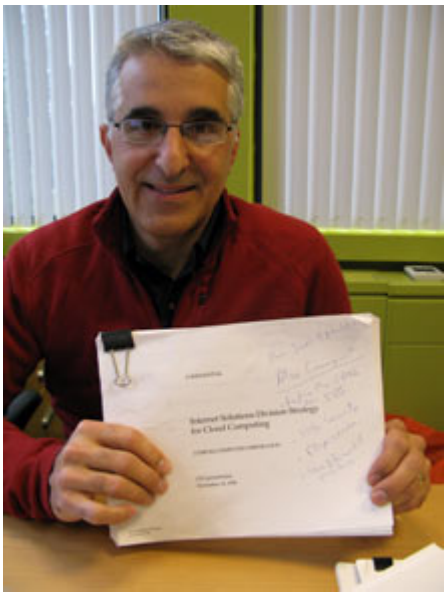
Who Coined 'Cloud Computing'?

Now that every technology company in America seems to be selling cloud computing, we decided to find out where it all began.

By Antonio Regalado

October 31, 2011

Cloud computing is one of the hottest buzzwords in technology. It appears 48 million times on the Internet. But amidst all the chatter, there is one question about cloud computing that has never been answered: Who said it first?



Proof of concept: George Favaloro poses with a 1996 Compaq business plan. The document is the earliest known use of the term “cloud computing” in print (click **here** to view).

Some accounts trace the birth of the term to 2006, when large companies such as Google and Amazon began using “cloud computing” to describe the new paradigm in which people are increasingly accessing software, computer power, and files over the Web instead of on their desktops.

But *Technology Review* tracked the coinage of the term back a decade earlier, to late 1996, and to an office park outside Houston. At the time, Netscape's Web browser was the technology to be excited about and the Yankees were playing Atlanta in the World Series. Inside the offices of Compaq Computer, a small group of technology executives was plotting the future of the Internet business and calling it "cloud computing."

Their vision was detailed and prescient. Not only would all business software move to the Web, but what they termed "cloud computing-enabled applications" like consumer file storage would become common. For two men in the room, a Compaq marketing executive named George Favaloro and a young technologist named Sean O'Sullivan, cloud computing would have dramatically different outcomes. For Compaq, it was the start of a $2-billion-a-year business selling servers to Internet providers. For O'Sullivan's startup venture, it was a step toward disenchantment and insolvency.

See the rest of our Business Impact report on Business in the Cloud.

Cloud computing still doesn't appear in the Oxford English Dictionary. But its use is spreading rapidly because it captures a historic shift in the IT industry as more computer memory, processing power, and apps are hosted in remote data centers, or the "cloud." With billions of dollars of IT spending in play, the term itself has become a disputed prize. In 2008, Dell drew outrage from programmers after attempting to win a trademark on "cloud computing." Other technology vendors, such as IBM and Oracle, have been accused of "cloud washing," or misusing the phrase to describe older product lines.

Like "Web 2.0," cloud computing has become a ubiquitous piece of jargon that many tech executives find annoying, but also hard to avoid. "I hated it, but I finally gave in," says Carl Bass, president and CEO of Autodesk, whose company unveiled a cloud-computing marketing campaign in September. "I didn't think the term helped explain anything to people who didn't already know what it is."

The U.S. government has also had trouble with the term. After the country's former IT czar, Vivek Kundra, pushed agencies to move to cheaper cloud services, procurement officials faced the question of what, exactly, counted as cloud computing. The government asked the National Institutes of Standards and Technology to come up with a definition. Its final draft, released this month, begins by cautioning that "cloud computing can and does mean different things to different people."

"The cloud is a metaphor for the Internet. It's a rebranding of the Internet," says Reuven Cohen, cofounder of Cloud Camp, a course for programmers. "That is why there is a raging debate. By virtue of being a metaphor, it's open to different interpretations." And, he adds, "it's worth money."

August 9, 2006, when then Google CEO Eric Schmidt introduced the term to an industry conference. "What's interesting [now] is that there is an emergent new model," Schmidt said, "I don't think people have really understood how big this opportunity really is. It starts with the premise that the data services and architecture should be on servers. We call it cloud computing—they should be in a "cloud" somewhere."

The term began to see wider use the following year, after companies including Amazon, Microsoft, and IBM started to tout cloud-computing efforts as well. That was also when it first appeared in newspaper articles, such as a *New York Times* report from November 15, 2007, that carried the headline "I.B.M. to Push 'Cloud Computing,' Using Data From Afar." It described vague plans for "Internet-based supercomputing."

Sam Johnston, director of cloud and IT services at Equinix, says cloud computing took hold among techies because it described something important. "We now had a common handle for a number of trends that we had been observing, such as the consumerization and commoditization of IT," he wrote in an e-mail.

Johnston says it's never been clear who coined the term. As an editor of the Wikipedia entry for cloud computing, Johnston keeps a close eye on any attempts at misappropriation. He was first to raise alarms about Dell's trademark application and this summer he removed a citation from Wikipedia saying a professor at Emory had coined the phrase in the late 1990s. There have been "many attempts to coopt the term, as well as various claims of invention," says Johnston.

That may explain why cloud watchers have generally disregarded or never learned of one unusually early usage—a May 1997 trademark application for "cloud computing" from a now-defunct company called NetCentric. The trademark application was for "educational services" such as "classes and seminars" and was never approved. But the use of the phrase was not coincidental. When *Technology Review* tracked down NetCentric's founder, O'Sullivan, he agreed to help dig up paper copies of 15-year-old business plans from NetCentric and Compaq. The documents, written in late 1996, not only extensively use the phrase "cloud computing," but also describe in accurate terms many of the ideas sweeping the Internet today.

Cloud 1.0: Entrepreneur Sean O'Sullivan filed a trademark on "cloud computing" in 1997. He poses at the offices of NetCentric, in Cambridge, Massachusetts during the late 1990s.

At the time, O'Sullivan's startup was negotiating a $5 million investment from Compaq, where Favaloro had recently been chosen to lead a new Internet services group. The group was a kind of internal "insurgency," recalls Favaloro, that aimed to get Compaq into the business of selling servers to Internet service providers, or ISPs, like AOL. NetCentric was a young company developing software that could help make that happen.

In their plans, the duo predicted technology trends that would take more than a decade to unfold. Copies of NetCentric's business plan contain an imaginary bill for "the total e-purchases" of one "George Favaloro," including $18.50 for 37 minutes of video conferencing and $4.95 for 253 megabytes of Internet storage (as well as $3.95 to view a Mike Tyson fight). Today, file storage and video are among the most used cloud-based applications, according to consultancy CDW. Back then, such services didn't exist. NetCentric's software platform was meant to allow ISPs to implement and bill for dozens, and ultimately thousands, of "cloud computing-enabled applications," according to the plan.

Exactly which of the men—Favaloro or O'Sullivan—came up with the term cloud computing remains uncertain. Neither recalls precisely when the phrase was conceived. Hard drives that would hold e-mails and other electronic clues from those precloud days are long gone.

Favaloro believes he coined the term. From a storage unit, he dug out a paper copy of a 50-page internal Compaq analysis titled "Internet Solutions Division Strategy for Cloud Computing" dated November 14, 1996. The document accurately predicts that enterprise software would give way to Web-enabled services, and that in the future, "application software is no longer a feature of the hardware—but of the Internet."

O'Sullivan thinks it could have been his idea—after all, why else would he later try to trademark it? He was also a constant presence at Compaq's Texas headquarters at the time. O'Sullivan located a daily planner, dated October 29, 1996, in which he had jotted down the phrase "Cloud Computing: The Cloud has no Borders" following a meeting with Favaloro that day. That handwritten note and the Compaq business plan, separated by two weeks, are the earliest documented references to the phrase "cloud computing" that *Technology Review* was able to locate.

"There are only two people who could have come up with the term: me, at NetCentric, or George Favaloro, at Compaq … or both of us together, brainstorming," says O'Sullivan.

Both agree that "cloud computing" was born as a marketing term. At the time, telecom networks were already referred to as the cloud; in engineering drawings, a cloud represented the network. What they were hunting for was a slogan to link the fast-developing Internet opportunity to businesses Compaq knew about. "Computing was bedrock for Compaq, but now this messy cloud was happening," says Favaloro. "And we needed a handle to bring those things together."

Their new marketing term didn't catch fire, however—and it's possible others independently coined the term at a later date. Consider the draft version of a January 1997 Compaq press release, announcing its investment in NetCentric, which described the deal as part of "a strategic initiative to provide 'Cloud Computing' to businesses." That phrase was destined to be ages ahead of its time, had not Compaq's internal PR team objected and changed it to "Internet computing" in the final version of the release.

In fact, Compaq eventually dropped the term entirely, along with its plans for Internet software. That didn't matter to Favaloro. He'd managed to point Compaq (which later merged with HP) toward what became a huge business selling servers to early Internet providers and Web-page hosters, like UUNet. "It's ridiculous now, but the big realization we had was that there was going to be an explosion of people using servers not on their premises," says Favaloro. "I went from being a heretic inside Compaq to being treated like a prophet."

For NetCentric, the cloud-computing concept ended in disappointment. O'Sullivan gave up using the term as he struggled to market an Internet fax service—one app the spotty network "cloud" of the day could handle. Eventually, the company went belly up and closed its doors. "We got drawn down a rathole, and we didn't end up launching a raft of cloud computing apps … that's something that sticks with me," says O'Sullivan, who later took a sabbatical from the tech world to attend film school and start a nonprofit to help with the reconstruction of Iraq.

company and, in terms of making us productive, our systems are far better than those of any of big company. We bring up and roll out new apps in a matter of hours. If we like them, we keep them, if not, we abandon them. We self-administer, everything meshes, we have access everywhere, it's safe, it's got great uptime, it's all backed up, and our costs are tiny," says Favaloro. "The vision came true."

by Antonio Regalado

KEEP READING

MOST POPULAR

This startup wants to copy you into an embryo for organ harvesting

With plans to create realistic synthetic embryos, grown in jars, Renewal Bio is on a journey to the horizon of science and ethics.

By Antonio Regalado

iCloud+ plans and pricing

When you sign up for iCloud, you automatically get 5GB of free storage. If you need more iCloud storage or want access to premium features, you can upgrade to iCloud+ .

About iCloud+

iCloud+ is Apple's premium cloud subscription. It gives you more storage for your photos, files, and backups, and additional features* available only to subscribers:

iCloud+ with 50GB storage

- 50GB of storage
- iCloud Private Relay (Beta)
- Hide My Email
- Custom Email Domain
- HomeKit Secure Video support for one camera

Share everything with up to five other family members.

iCloud+ with 200GB storage

- 200GB of storage
- iCloud Private Relay (Beta)
- Hide My Email
- Custom Email Domain
- HomeKit Secure Video support for up to five cameras

Share everything with up to five other family members.

iCloud+ with 2TB storage

- 2TB of storage
- iCloud Private Relay (Beta)
- Hide My Email
- Custom Email Domain
- HomeKit Secure Video support for an unlimited number of cameras

Share everything with up to five other family members.

You can upgrade to iCloud+ from your iPhone, iPad, iPod touch, Mac, or PC. After you upgrade, you'll be billed monthly.[1] See the monthly pricing and plans per country or region below.

* Not all features are available in all countries or regions. HomeKit Secure Video requires a supported iCloud plan, compatible HomeKit-enabled security camera, and HomePod, Apple TV, or iPad running as a home hub. Private Relay is currently in beta. Some websites might have issues like showing content for the wrong region or requiring extra steps to sign in.

iCloud+ pricing

- North America, South America, Latin America, and the Caribbean
- Europe, the Middle East, and Africa
- Asia Pacific

North America, South America, Latin America, and the Caribbean

Brazil (BRL)
50GB: R$ 3.50
200GB: R$ 10.90
2TB: R$ 34.90

Colombia (COP)
50GB: $2800
200GB: $8500
2TB: $27900

Peru (PEN)
50GB: S/.2.90
200GB: S/.9.90
2TB: S/.29.90

Canada (CAD)
50GB: $1.29
200GB: $3.99
2TB: $12.99

Mexico (MXN)
50GB: $17
200GB: $49
2TB: $179

United States[4] (USD)
50GB: $0.99
200GB: $2.99
2TB: $9.99

Chile (CLP)
50GB: $650
200GB: $1900
2TB: $6500

Europe, the Middle East, and Africa

Albania[2,3] (USD)
50GB: $1.19
200GB: $3.59
2TB: $11.99

Hungary[3] (HUF)
50GB: 299 Ft
200GB: 899 Ft
2TB: 2990 Ft

Russia[3] (RUB)
50GB: 59 р.
200GB: 149 р.
2TB: 599 р.

Armenia[2,3]
50GB: $1.19
200GB: $3.49
2TB: $11.99

Iceland[2,3] (USD)
50GB: $1.23
200GB: $3.71
2TB: $12.39

Saudi Arabia[3] (SAR)
50GB: 3.69ريال
200GB: 10.99ريال
2TB: 36.99ريال

Belarus[2,3] (USD)
50GB: $1.19
200GB: $3.49
2TB: $11.99

Israel (ILS)
50GB: ₪3.90
200GB: ₪11.90
2TB: ₪39.90

South Africa[3] (ZAR)
50GB: R14.99
200GB: R44.99
2TB: R149.99

Bulgaria[3] (BGN)
50GB: 1.99 лв
200GB: 5.99 лв
2TB: 18.99 лв

Nigeria (NGN)
50GB: ₦300
200GB: ₦900
2TB: ₦2900

Sweden[3] (SEK)
50GB: 9 kr
200GB: 29 kr
2TB: 89 kr

Croatia[3] (HRK)
50GB: 7.99 kn (0.99 €)
200GB: 24.99 kn (2.99 €)
2TB: 79.99 kn (9.99 €)

Norway[3] (NOK)
50GB: 10 kr
200GB: 29 kr
2TB: 99 kr

Switzerland[3] (CHF)
50GB: CHF 1
200GB: CHF 3
2TB: CHF 10

Czech Republic[3] (CZK)
50GB: 25 Kč
200GB: 79 Kč
2TB: 249 Kč

Pakistan (PKR)
50GB: Rs100
200GB: Rs300
2TB: Rs1000

Tanzania (TZS)
50GB: 1900 TSh
200GB: 5900 TSh
2TB: 19900 TSh

Denmark[3] (DKK)
50GB: 7 kr
200GB: 25 kr
2TB: 69 kr

Poland[3] (PLN)
50GB: 3.99 zł
200GB: 11.99 zł
2TB: 39.99 zł

Turkey[3] (TRY)
50GB: 6.49 TL
200GB: 19.99 TL
2TB: 64.99 TL

Egypt[3] (EGP)
50GB: £18.99
200GB: £54.99
2TB: £189.99

Qatar (QAR)
50GB: 3.69ريال
200GB: 10.99ريال
2TB: 36.99ريال

United Arab Emirates[3] (AED)
50GB: AED 3.69
200GB: AED 10.99
2TB: AED 36.99

Euro[3] (Euro)
50GB: 0.99 €
200GB: 2.99 €
2TB: 9.99 €

Romania[3] (RON)
50GB: 4.49 lei
200GB: 12.99 lei
2TB: 44.99 lei

United Kingdom[3] (GBP)
50GB: £0.79
200GB: £2.49
2TB: £6.99

Asia Pacific

Australia[3] (AUD)
50GB: $1.49
200GB: $4.49
2TB: $14.99

Japan[3] (JPY)
50GB: ¥130
200GB: ¥400
2TB: ¥1300

Republic of Korea (KRW)
50GB: ₩1,100
200GB: ₩3,300
2TB: ₩11,100

China mainland[3] (CNY)
50GB: ¥6
200GB: ¥21
2TB: ¥68

Kazakhstan (KZT)
50GB: ₸349
200GB: ₸999
2TB: ₸3490

Singapore (SGD)
50GB: S$ 1.28
200GB: S$ 3.98
2TB: S$ 12.98

Hong Kong (HKD)
50GB: HK$ 8
200GB: HK$ 23
2TB: HK$ 78

Malaysia (MYR)
50GB: RM3.90
200GB: RM11.90
2TB: RM39.90

Taiwan[3] (TWD)
50GB: NT$ 30
200GB: NT$ 90
2TB: NT$ 300

India[3] (INR)
50GB: Rs 75
200GB: Rs 219
2TB: Rs 749

New Zealand[3] (NZD)
50GB: $1.69
200GB: $4.99
2TB: $16.99

Thailand (THB)
50GB: ฿35
200GB: ฿99
2TB: ฿349

Indonesia (IDR)
50GB: Rp 15000
200GB: Rp 45000
2TB: Rp 149000

Philippines (PHP)
50GB: ₱49
200GB: ₱149
2TB: ₱499

Vietnam (VND)
50GB: ₫19000
200GB: ₫59000
2TB: ₫199000

1. For countries and regions where the local currency isn't supported, such as Argentina, storage upgrades are billed in U.S. dollars (USD). Learn more about countries and regions that bill in U.S. dollars (USD).

2. iCloud+ upgrades for Albania, Armenia, Belarus, and Iceland are charged in U.S. dollars (USD), with prices slightly higher due to the Value Added Tax (VAT).

3. Taxes are included in all prices for these countries and regions: Albania, Armenia, Australia, Austria, Belarus, Belgium, Bulgaria, China mainland, Croatia, Cyprus, Czech Republic, Denmark, Egypt, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, India, Ireland, Italy, Japan, Republic of Korea, Latvia, Lithuania, Luxembourg, Malta, Netherlands, New Zealand, Norway, Poland, Portugal, Romania, Russia, Saudi Arabia, Slovakia, Slovenia, South Africa, Spain, Sweden, Switzerland, Taiwan, Turkey, the United Arab Emirates, and the United Kingdom.

4. Residents in some U.S. states have tax added to the monthly payment due to state laws.

Accepted payment methods for iCloud+ upgrades include credit cards, debit cards, and your Apple Account balance. If you don't have enough available funds in your Apple Account balance to complete your upgrade, you'll be charged the remaining amount. Apple Store gift cards aren't accepted as payment for upgrading iCloud+. Learn how to manage the amount of storage you're using.

Learn how iCloud operates in China mainland.

Published Date: September 01, 2022

Related topics

Download iCloud for Windows ›

Downgrade or cancel your iCloud+ plan ›

About iCloud Private Relay ›

Start a discussion in Apple Support Communities

Ask other users about this article

Submit my question

See all questions on this article ›

Contact Apple Support

Need more help? Save time by starting your support request online and we'll connect you to an expert.

Get started ›

Dropbox

Sign in

Choose the right Dropbox for you

Billed monthly Billed yearly **(Save up to 20%)**

For individuals	For households	For solo-workers
Plus	**Family**	**Professional**
$9.99 / month	**$16.99 / family / month**	**$16.58 / month**
2 TB (2,000 GB) • 1 user	Shared 2 TB (2,000 GB) • Up to 6 users	3 TB (3,000 GB) • 1 user
Buy now	Buy now	Try for free
		or purchase now
✓ Unlimited device linking	**Everything in Plus, and:**	**Everything in Plus, and:**
✓ 30-day file and account recovery	✓ Individual accounts for up to 6 people	✓ 180-day file and account recovery
✓ Large file delivery with Dropbox Transfer (up to 2 GB)	✓ Access to Family Room folder for easy group sharing and coordination	✓ Advanced sharing controls and file locking
✓ 3 free eSignatures per month	✓ A single bill for the whole family	✓ Large file delivery with Dropbox Transfer (up to 100 GB, including customization options)

For growing teams

Standard

$15 / user / month

Shared 5 TB (5,000 GB) • 3+ users

Try for free

or purchase now

- Easy to use content protection and external sharing controls
- Recover files or restore your entire account up to 180 days
- Automatically back up computers—and connected external drives—directly to the cloud

For complex teams

Advanced

$24 / user / month

As much space as needed • 3+ users

Try for free

or purchase now

Everything in Standard, and:

- Always-on security monitoring, notifications, and alerts
- Large file delivery with Dropbox Transfer (up to 100 GB, including customization options)
- Ransomware detection and recovery

For large organizations

Enterprise

Contact sales for pricing

As much space as needed • 3+ users

Contact us

Everything in Advanced, and:

- Enterprise-grade security and visibility tools
- Integrations with best-in-class security solutions
- Dedicated customer success manager

Compare all features ↓

Just need 2 GB to store and share your files?

Sign up for our free plan

Compare all features

	Personal		Business		
	Plus For individuals Buy now	Family For families Buy now	Professional For individuals Try for free or purchase now	Standard For growing teams Try for free or purchase now	Advanced For complex teams Try for free or purchase now
Dropbox core features					
					As much space as

Storage	2,000 GB	Share 2,000 GB	3,000 GB	5,000 GB	needed
Users	1 user	Up to 6 users	1 user	3+ users	3+ users
Best-in-class sync technology	✓	✓	✓	✓	✓
Anytime, anywhere access	✓	✓	✓	✓	✓
Easy and secure sharing	✓	✓	✓	✓	✓
256-bit AES and SSL/TLS encryption	✓	✓	✓	✓	✓
Content and accident protection					
Dropbox Backup	✓	✓	✓	✓	✓
File recovery and version history	30 days	30 days	180 days	180 days	1 year
Dropbox Rewind	30-day history	30-day history	180-day history	180-day history	1-year history
Shared link controls	✗	✗	✓	✓	✓
External sharing controls and reporting	✗	✗	✗	✓	✓
Data Classification	✗	✗	✗	✗	✓
Ransomware detection and recovery	✗	✗	✗	✗	✓
Alerts and notifications	✗	✗	✗	✗	✓
Dropbox Passwords	✓	✓	✓	✓	✓
Dropbox Vault	✓	✓	✓	✗	✗
Watermarking	✗	✗	✓	✓	✓
Account transfer tool	✗	✗	✗	✓	✓
Enable multi-factor authentication	✓	✓	✓	✓	✓
Enables HIPAA compliance	✗	✗	✗	✓	✓

Aa13

Remote device wipe	✓	✓	✓	✓	✓
Device approvals	✗	✗	✗	✓	✓
Productivity and sharing tools					
Family Room	✗	✓	✗	✗	✗
Dropbox Paper	✓	✓	✓	✓	✓
Dropbox Transfer	Send up to 2 GB per Transfer	Send up to 2 GB per Transfer	Send up to 100 GB per Transfer, including customization options	Send up to 2 GB per Transfer	Send up to 100 GB per Transfer, including customization options
HelloSign eSignatures	Send up to 3 documents for eSignature per month	Send up to 3 documents for eSignature per month	Send up to 3 documents for eSignature per month * **Unlimited eSignature bundle available*	Send up to 3 documents for eSignature per month	Send up to 3 documents for eSignature per month
File locking	✗	✗	✓	✓	✓
Integrated cloud content	✓	✓	✓	✓	✓
Branded sharing	✗	✗	✓	✓	✓
Web previews and comments	✓	✓	✓	✓	✓
Plus button	✓	✓	✓	✓	✓
File requests	✓	✓	✓	✓	✓
Full text search	✓	✓	✓	✓	✓
Viewer history	✗	✗	✓	✗	✓
Team management					
Admin console	✗	✗	✗	✓	✓
Multi-team admin login	✗	✗	✗	✓	✓
Centralized billing	✗	✓	✗	✓	✓

Company-managed groups	✗	✗	✗	✓	✓
Unlimited API access to security platform partners	✗	✗	✗	✓	✓
Unlimited API access to productivity platform partners	✓	✓	✓	✓	✓
1 billion API calls/month for data transport partners	✗	✗	✗	✓	✓
Tiered admin roles	✗	✗	✗	✗	✓
Sign in as user	✗	✗	✗	✗	✓
Audit logs with file event tracking	✗	✗	✗	✗	✓
Single sign-on (SSO) integrations	✗	✗	✗	✗	✓
Invite enforcement	✗	✗	✗	✗	✓
Support					
Priority email support	✓	✓	✓	✓	✓
Live chat support	✓	✓	✓	✓	✓
Phone support during business hours	✗	✗	✗	✓	✓
	For individuals	For families	For individuals	For growing teams	For complex teams

Experience Dropbox

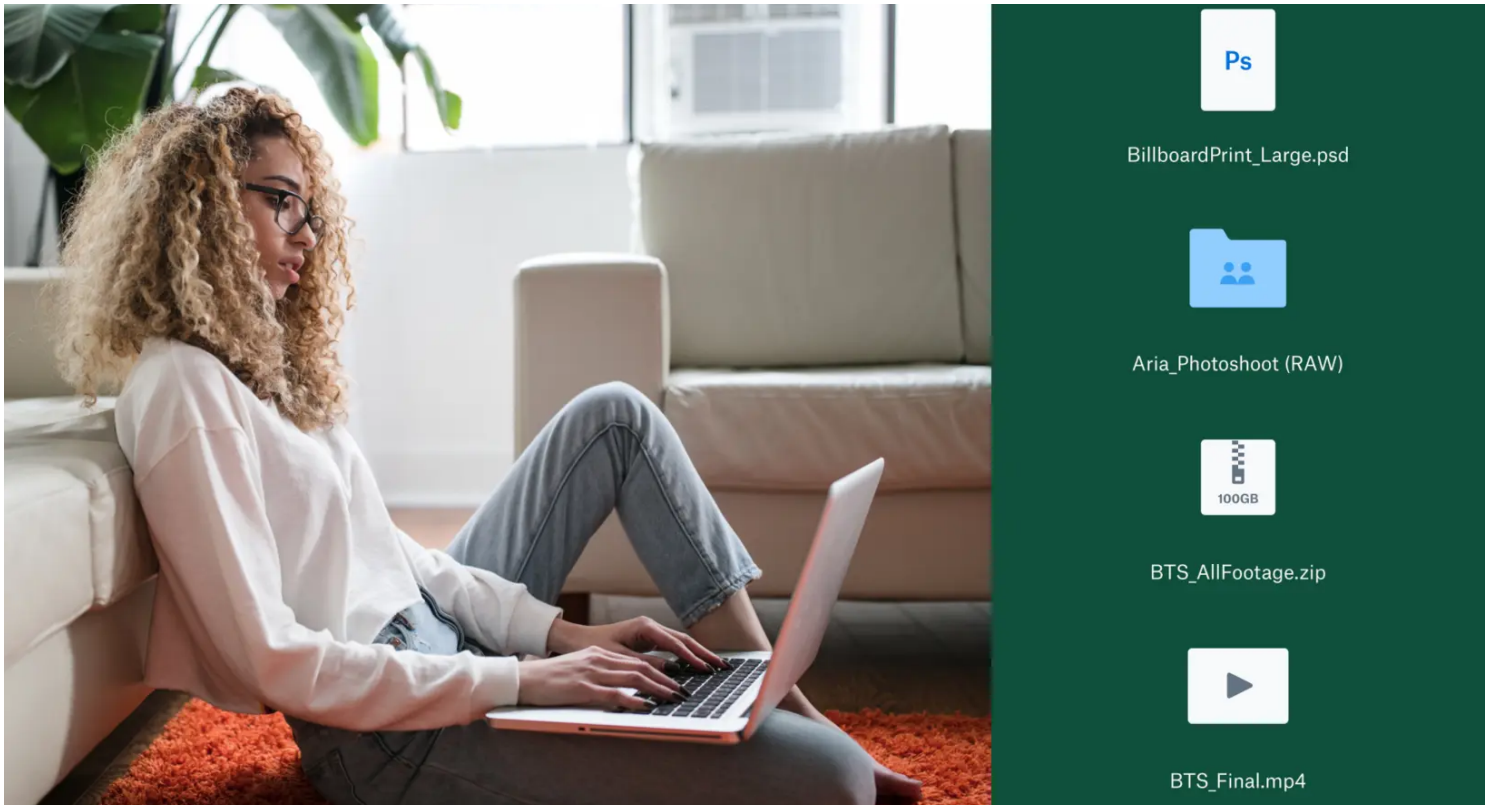
Search

How much is 1 TB of storage?

1 TB of storage equals 1,000 GB of data—that's about 16 entry-level smartphones.

Share this

Compare cloud storage plans



What is a terabyte?

When talking about data storage, we often measure whole system storage capacity in terabytes, but most individual files take up megabytes or gigabytes for large files. So how many gigabytes or megabytes are in a terabyte? 1 TB equals 1,000 gigabytes (GB) or 1,000,000 megabytes (MB).

Aa16

individual external hard drives often start at 1 TB of storage, with larger options going past 32 TB.

How much data can 1 TB hold?

The average user stores a mix of photos, videos, and documents. When you're setting up a cloud storage plan, it's hard to gauge how many photos and videos 1 TB of data can hold. One terabyte gives you the option of storing roughly:

- 250,000 photos taken with a 12MP camera;
- 250 movies or 500 hours of HD video; or
- 6.5 million document pages, commonly stored as Office files, PDFs, and presentations. It's also equal to 1,300 physical filing cabinets of paper!

Store it all in cloud storage

If your phone runs out of space, you're probably not carrying around a second one. When you're running out of storage space on your Apple or Microsoft computer, clunky portable hard drives are fragile, and small flash drives are easy to lose. Plus, the way you connect them to a computer seems to change every year. Your old external USB 3.0 hard drive won't work with a new computer that only has USB-C ports unless you get a special adaptor.

The cloud gives you an easier way to store a large amount of data, including photos, videos, and important files, without ever having to worry about disk space. When you store content in the cloud, you'll be able to do more with it, like:

- Store everything without being picky about what you save. It's also a good idea to follow the 3-2-1 rule: 3 copies of a file on 2 separate medias, with 1 copy off site.
- Access files or work remotely, whenever it's needed—even from mobile devices

Is 1 TB enough data for you?

- Dropbox Plus comes with 2 TB of storage (for 1 user)
- Dropbox Family comes with 2 TB of storage (for up to 6 users)
- Dropbox Professional has 3 TB of storage
- Dropbox Standard, Advanced, and Enterprise starts at 5 TB of storage (or as much storage as you need depending on your plan) so you don't fret about space

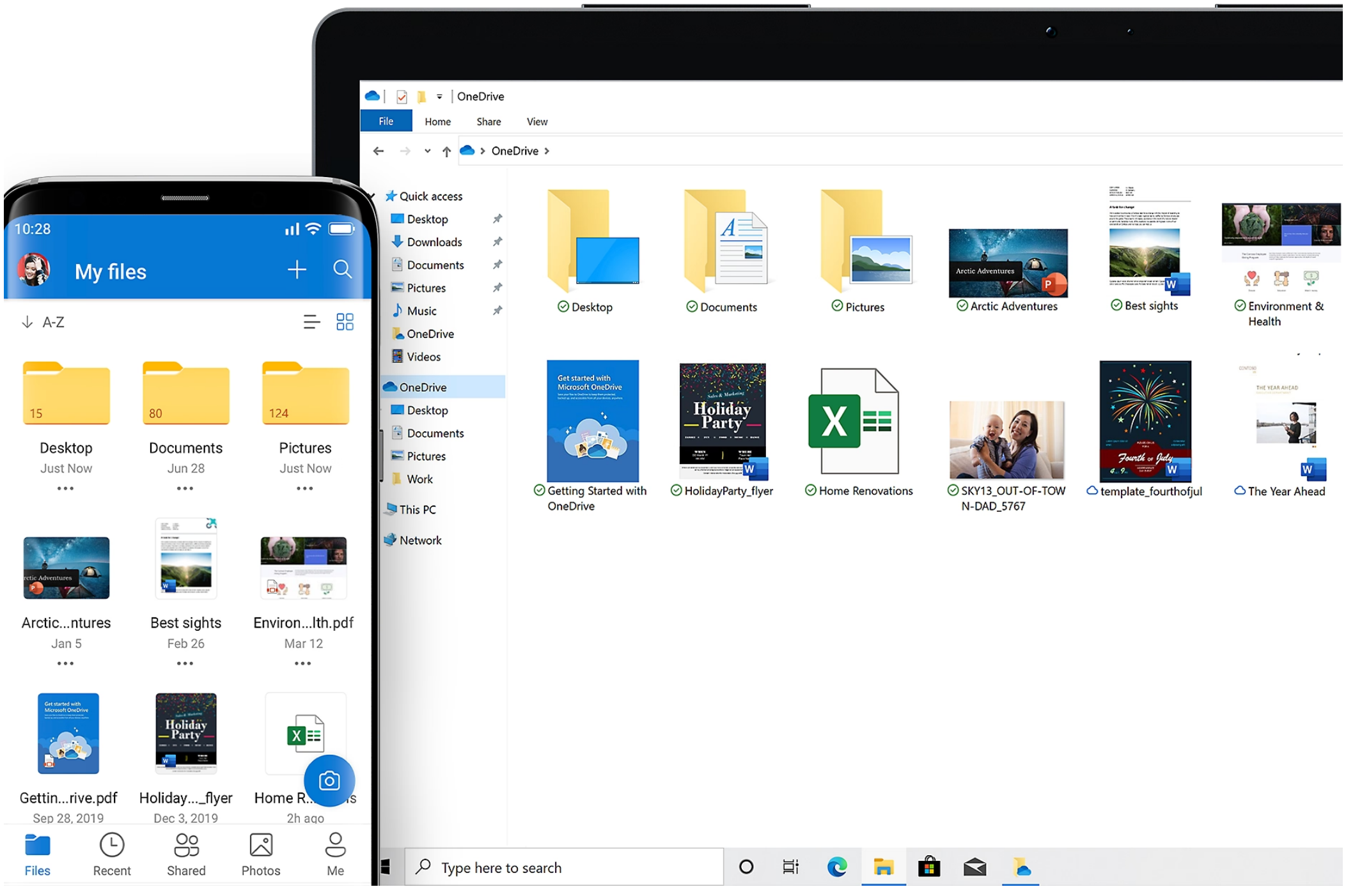
Microsoft | Microsoft 365 Products All Microsoft

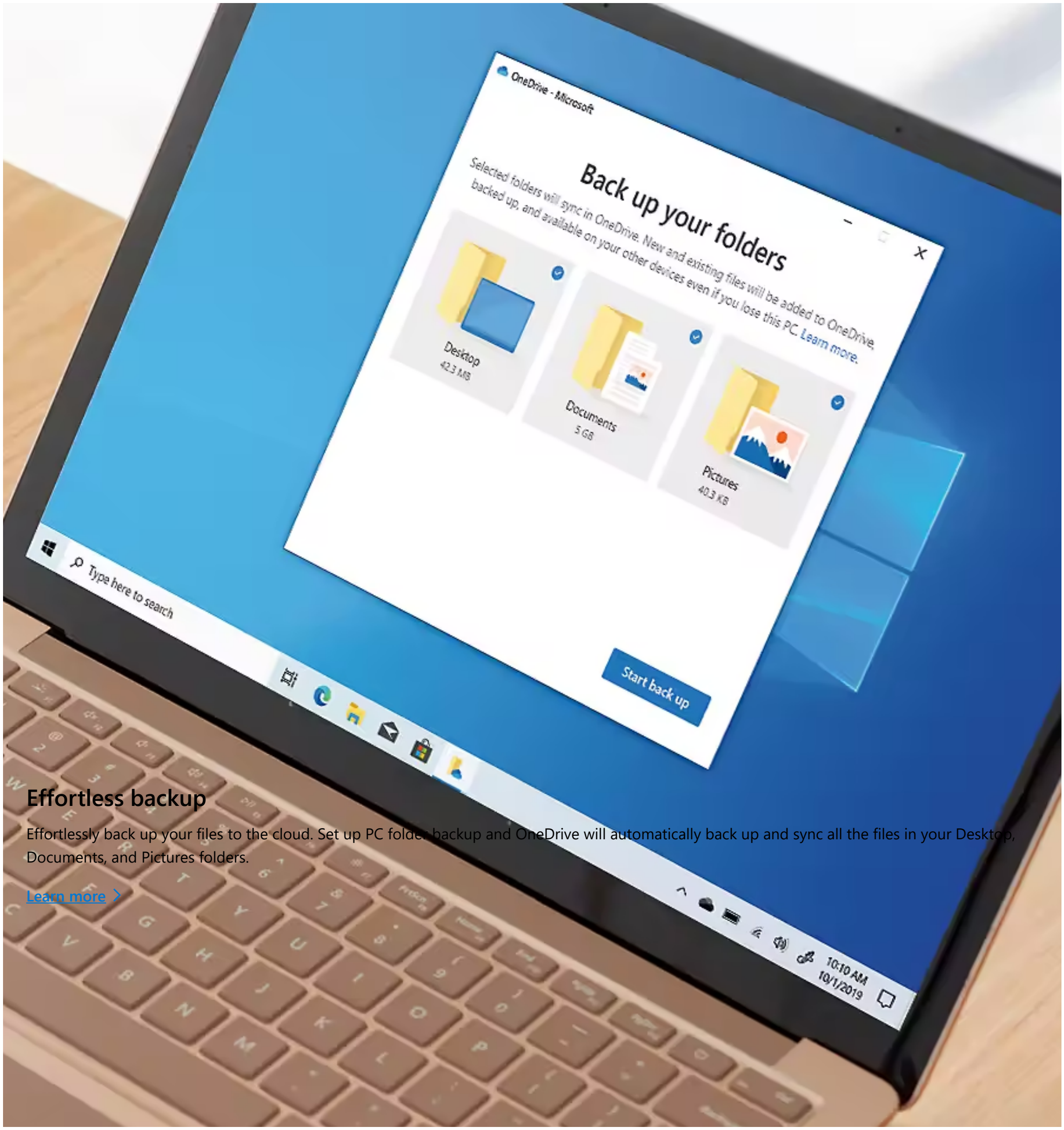
OneDrive PC folder backup

PC folder backup automatically syncs your Desktop, Documents and Pictures folders on your Windows PC to your OneDrive cloud storage. Your files and folders stay protected and are available from any device.

Get started | See it in action

Don't have OneDrive? Get the free desktop app





Effortless backup

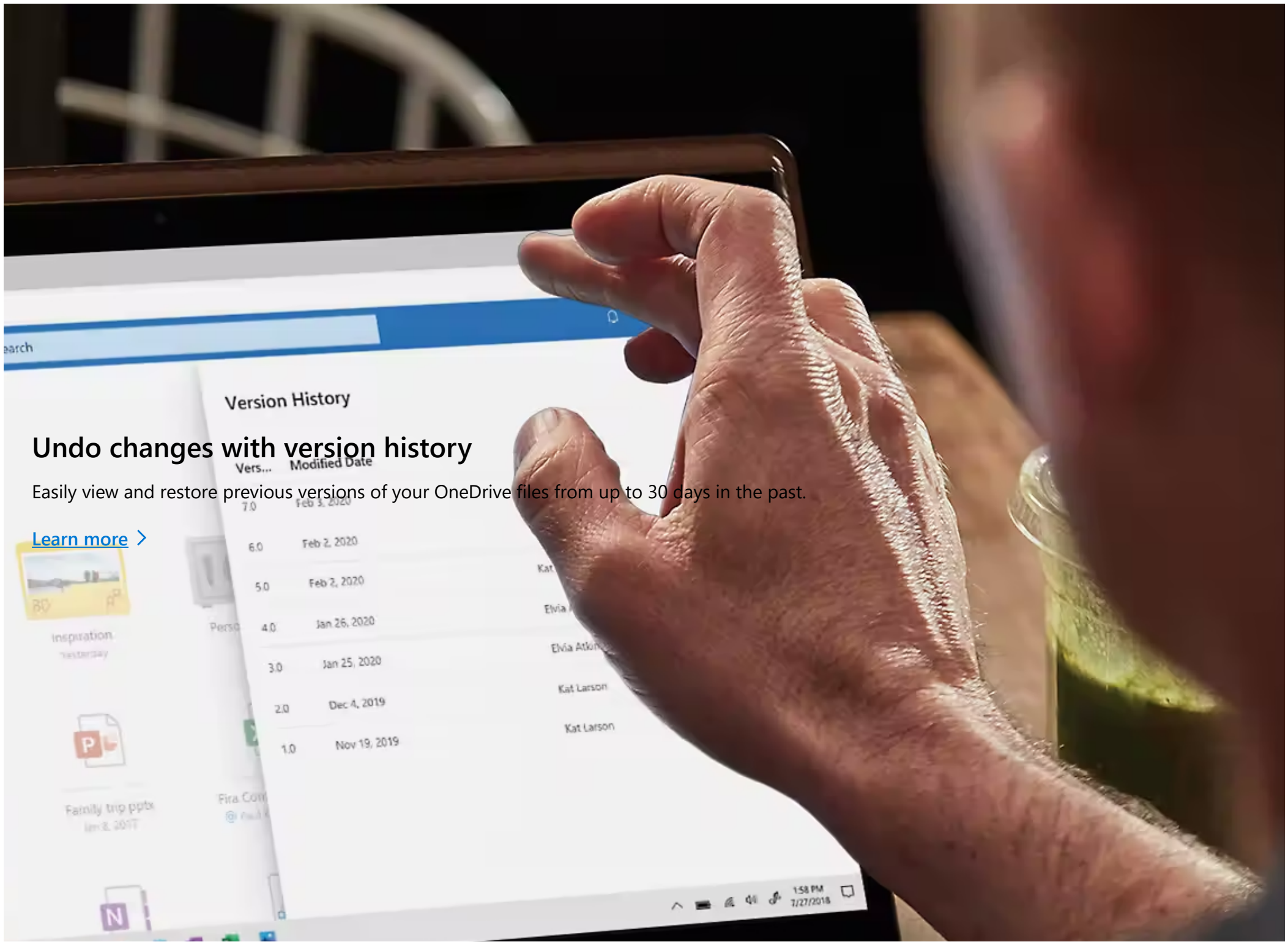
Effortlessly back up your files to the cloud. Set up PC folder backup and OneDrive will automatically back up and sync all the files in your Desktop, Documents, and Pictures folders.

Learn more >

Access your PC files without your PC

Your backed-up PC folders are available online and in the OneDrive mobile app for you to view or edit files on the go.

Get the mobile app >

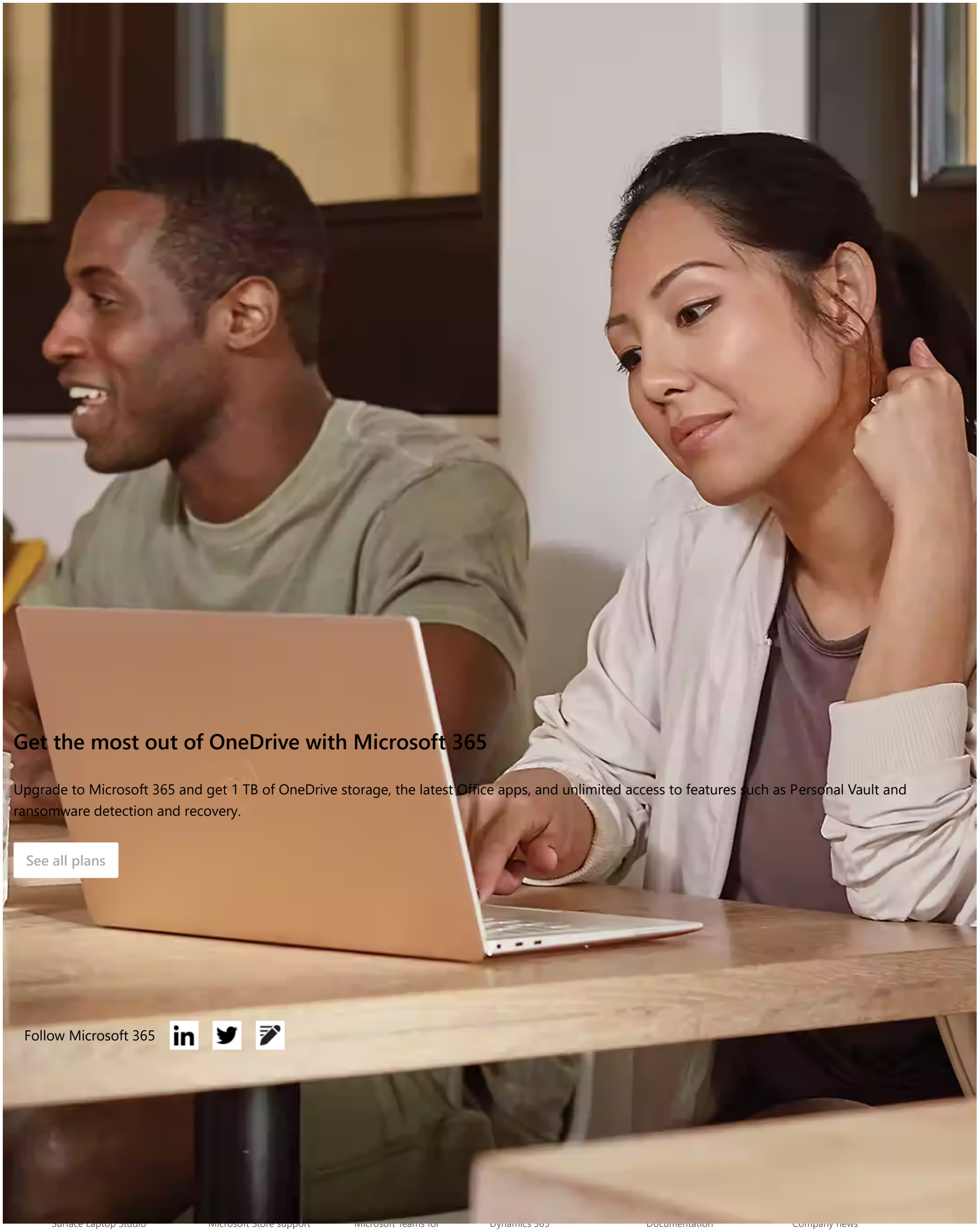


Protect files from ransomware attacks

With a Microsoft 365 subscription, OneDrive will detect ransomware attacks and help restore your files up to 30 days after the attack.

Learn more

Aa22



Surface Laptop Studio
Surface Pro X
Surface Go 3
Surface Duo 2
Surface Pro 7+
Windows 11 apps

Microsoft Store support
Returns
Order tracking
Virtual workshops and training
Microsoft Store Promise
Flexible Payments

Microsoft Teams for Education
Microsoft 365 Education
Education consultation appointment
Educator training and development
Deals for students and parents

Dynamics 365
Microsoft 365
Microsoft Power Platform
Microsoft Teams
Microsoft Industry
Small Business

Documentation
Microsoft Learn
Microsoft Tech Community
Azure Marketplace
AppSource
Visual Studio

Company news
Privacy at Microsoft
Investors
Diversity and inclusion
Accessibility
Sustainability

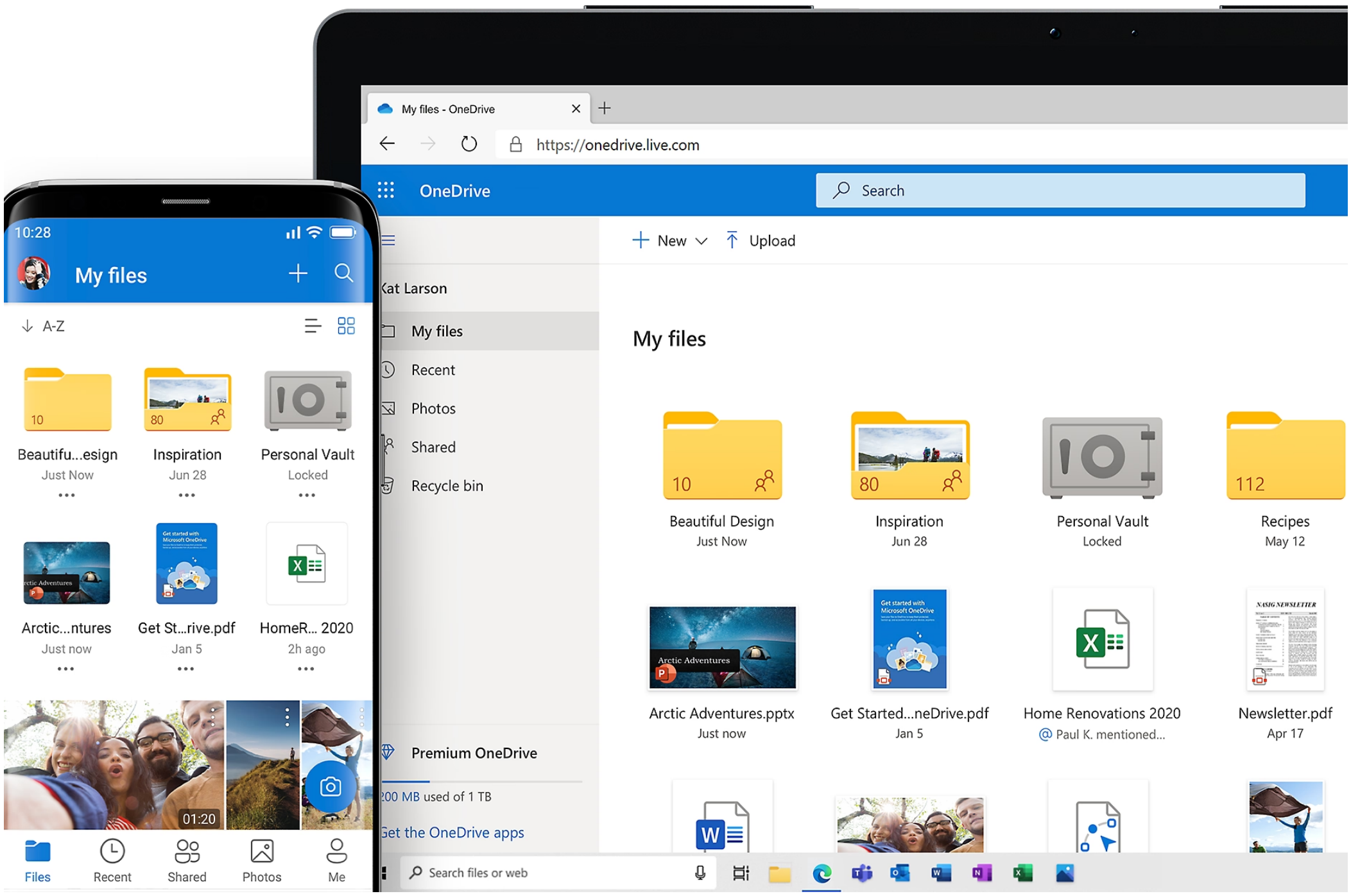
Aa23

OneDrive Personal Cloud Storage

Save your photos and files to OneDrive and access them from any device, anywhere.

Create free account | See plans and pricing

Already have OneDrive? Sign in >



Organized. Protected. Connected.

Anywhere access

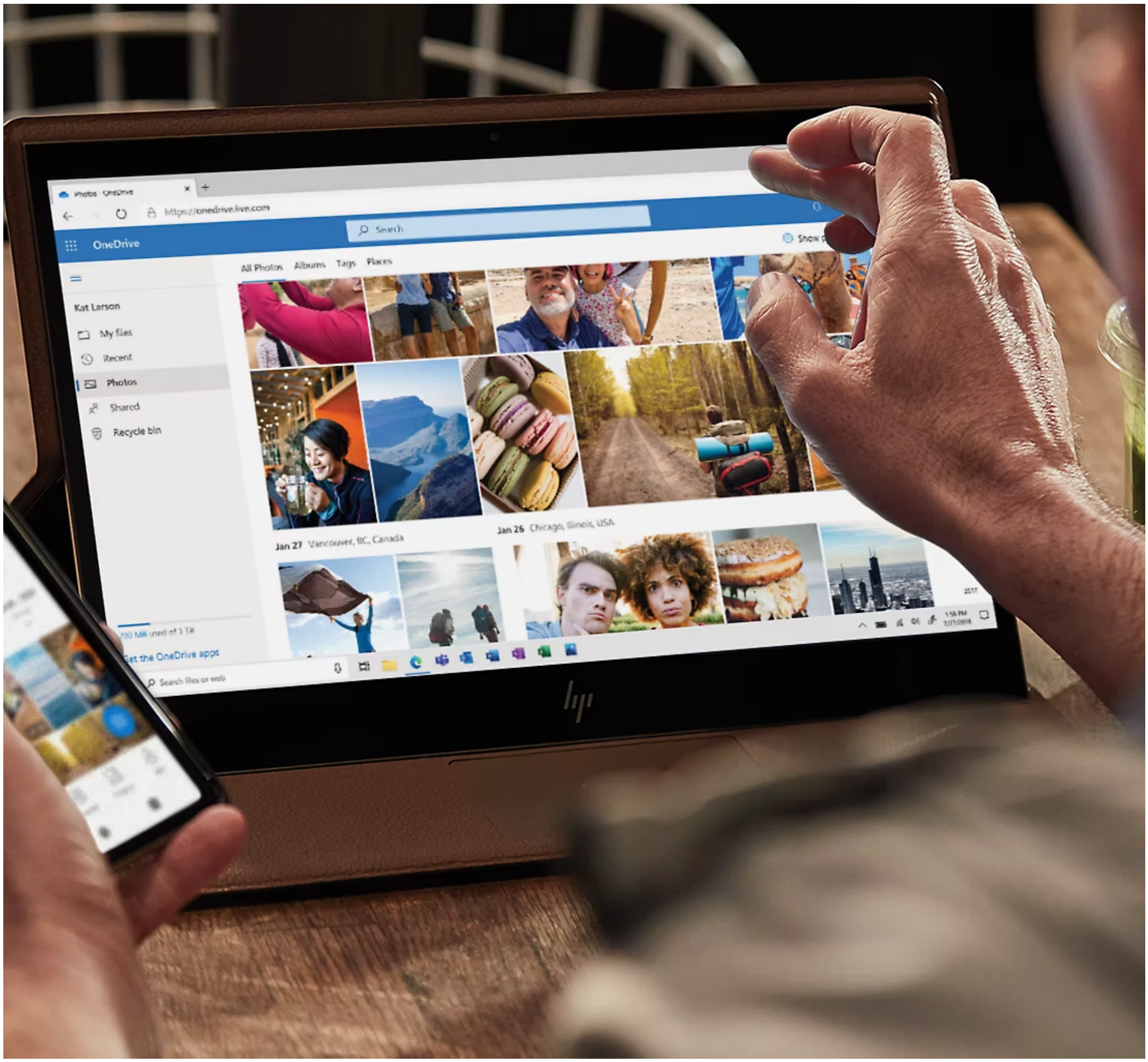
Enjoy the freedom to access, edit, and share your files on all your devices, wherever you are.

Back up and protect

If you lose your device, you won't lose your files and photos when they're saved in OneDrive.

Share and collaborate

Stay connected, share your documents and photos with friends and family, and collaborate in real time with Office apps.



Share and collaborate

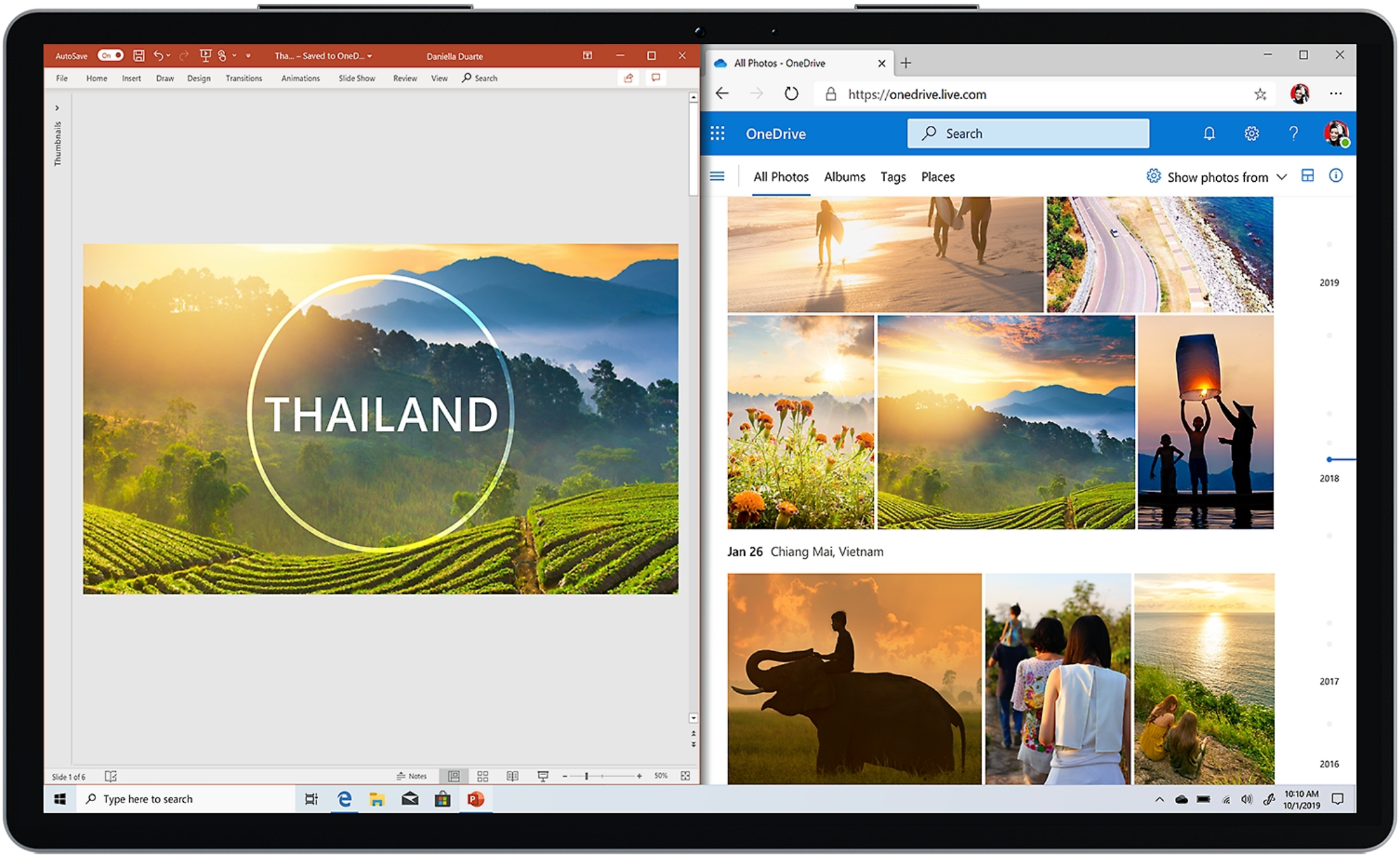
Share files, folders, and photos with friends and family. No more large email attachments or thumb drives—just send a link via email or text.

Download Microsoft OneDrive mobile app >

Get more done with Microsoft 365

Create your best work with the latest versions of Word, Excel, and other Office apps. Plus, get 1 TB of cloud storage, document sharing, ransomware recovery, and more with OneDrive.

Learn more >



Features to make life easier and safer

Aa26

Files on demand

Access all your OneDrive files in Windows 11 without taking up space on your PC.

Document scanning

Use your mobile device to scan and store documents, receipts, business cards, notes, and more in OneDrive.

Personal Vault

Store important files and photos with an added layer of protection in OneDrive Personal Vault.

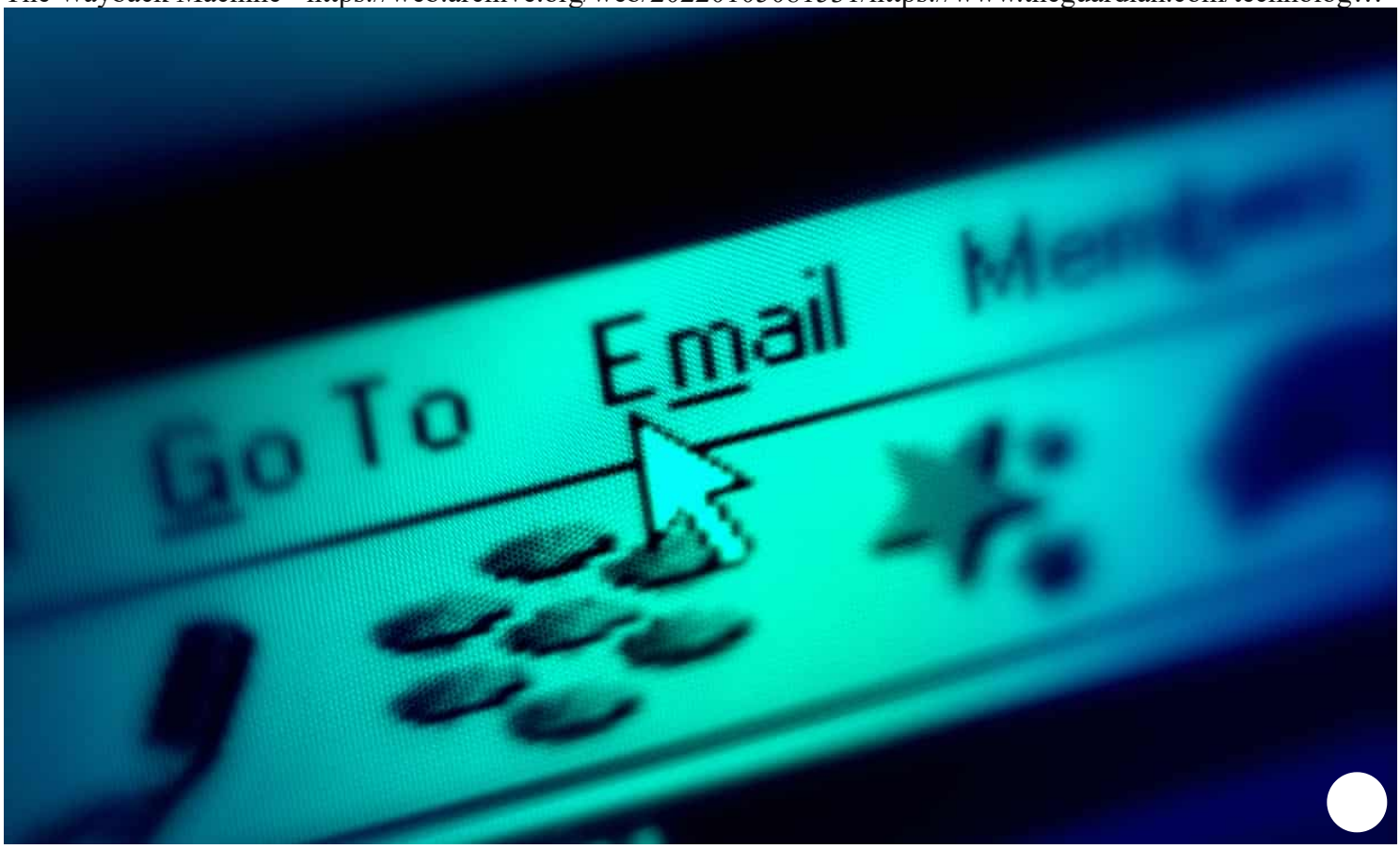
Access your photos and files on all your devices

Sign in

See plans and pricing

Follow Microsoft 365

Aa27



Internet

How did email grow from messages between academics to a global epidemic?

Ray Tomlinson, the man who literally put the @ in email addresses, has died. Here's a brief history of electronic messages, from the Queen's first mail to the triumph of spam

Samuel Gibbs

Mon 7 Mar 2016 10.07 EST

Ray Tomlinson, the man who literally put the "@" in email, died on Saturday, but his invention, which allowed electronic messages to spread across the internet and fill our lives and our inboxes on a daily basis, will live on.

Here is a brief look at what Tomlinson started and the evolution of email through the last half-century.

The first electronic message - 1965

Computers were all about spools of paper and tape back when the first email was sent in the 1960s. Photograph: H. Armstrong Roberts/ClassicStock/Corbis

The very first version of what would become known as email was invented in 1965 at Massachusetts Institute of Technology (MIT) as part of the university's Compatible Time-Sharing System, which allowed users to share files and messages on a central disk, logging in from remote terminals.

Tomlinson and the @ - 1971

The man who quite literally put the @ sign at the heart of email. Photograph: Handout

American computer programmer Tomlinson arguably conceived the method of sending email between different computers across the forerunner to the internet, Arpanet, at the US Defense Advanced Research Projects Agency (Darpa), introducing the "@" sign to allow messages to be targeted at certain users on certain machines.

Emails become a standard - 1973

Before they were commissioning robots for the battlefield, Darpa started with the internet and email. Photograph: HO/AFP/Getty Images

The first email standard was proposed in 1973 at Darpa and finalised within Arpanet in 1977, including common things such as the to and from fields, and the ability to forward emails to others who were not initially a recipient.

The Queen sends her first email - 1976

If the Queen had known what email would do to the popularity of her beloved stamps, would she have pressed send? Photograph: Martin Keene/PA

Queen Elizabeth II sends an email on Arpanet, becoming the first head of state to do so.

Eric Schmidt designs BerkNet - 1978

Before Google, Schmidt developed one of the first intranet systems and messaging over serial connections in the world as part of his degree. Photograph: Scott Olson/Getty Images

Eric Schmidt, who would later lead Google and oversee the introduction of Gmail, wrote Berkley Network as part of his master's thesis in 1978, which was an early intranet service offering messaging over serial connections.

EMAIL program developed - 1979

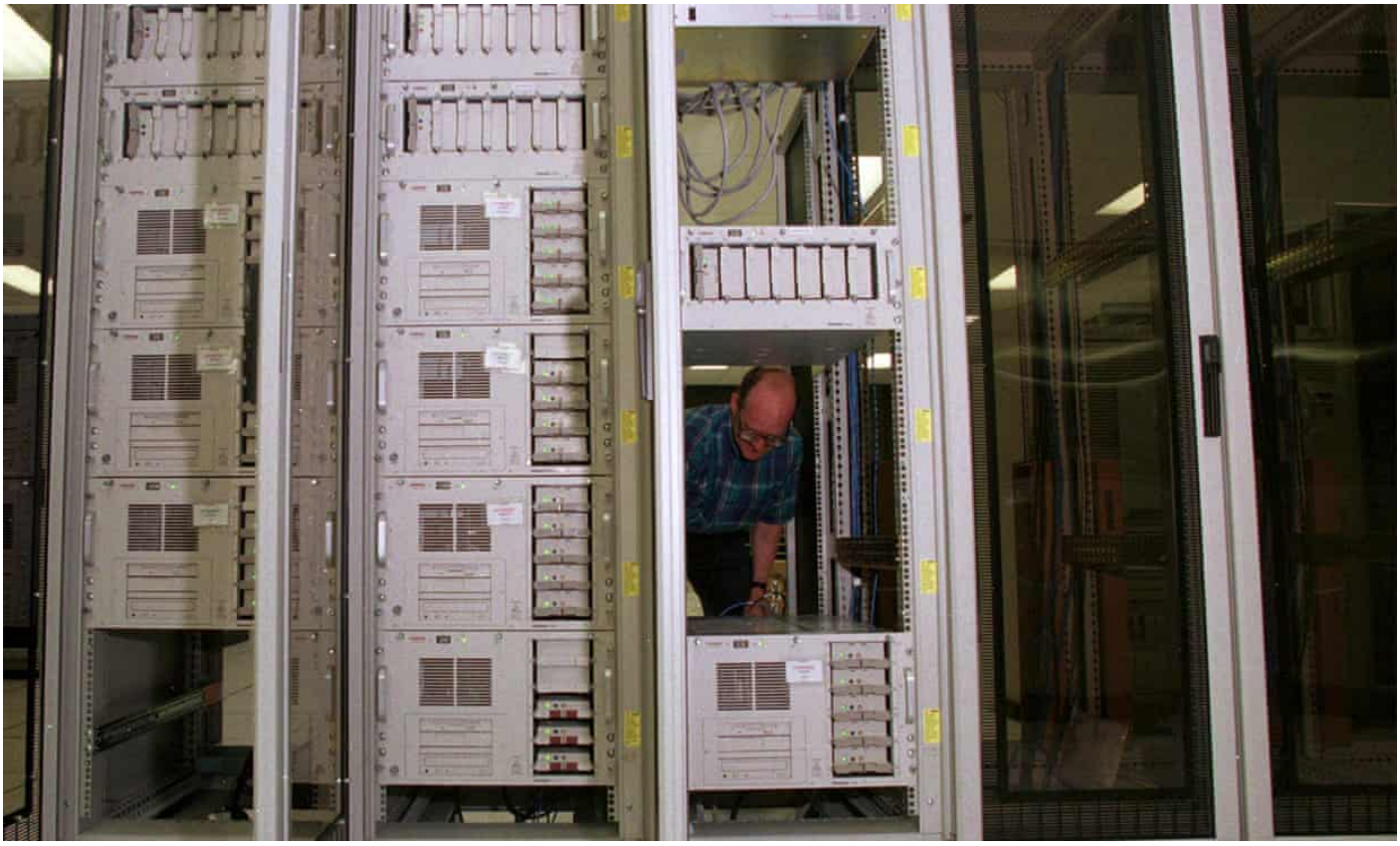
At the age of 14, Shiva Ayyadurai writes a program called EMAIL for the University of Medicine and Dentistry of New Jersey, which sent electronic messages within the university, later copyrighting the term in 1982. Whether or not this is the first use of the word email is up for debate.

Microsoft Mail arrives - 1988

'Calm down guys, I'm sure this email thing won't catch on. Photograph: Lou Dematteis/Reuters

The first version of Microsoft Mail was released in 1988 for Mac OS, allowing users of Apple's AppleTalk Networks to send messages to each other. In 1991, a second version was released for other platforms including DOS and Windows, which laid the groundwork for Microsoft's later Outlook and Exchange email systems.

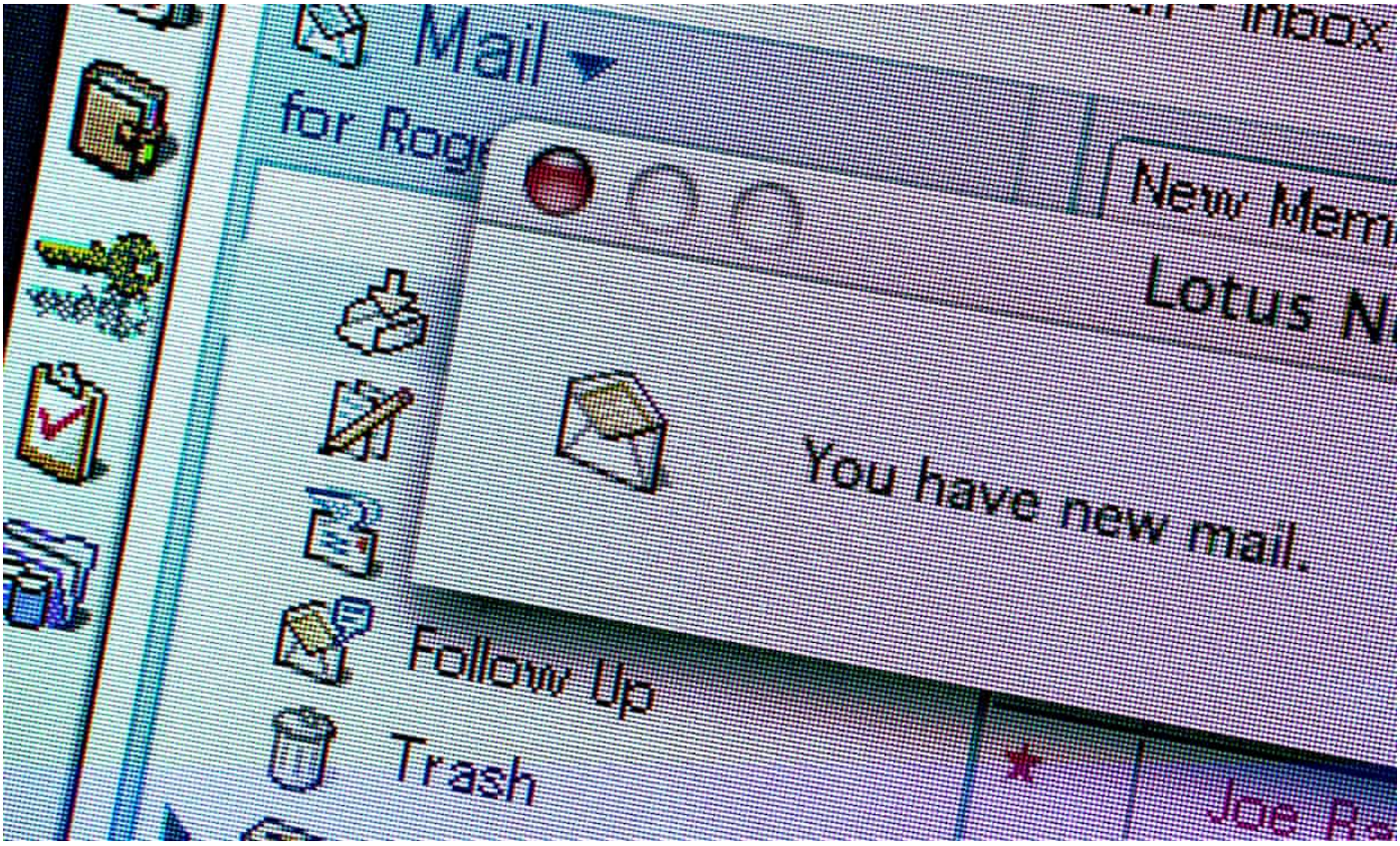
CompuServe starts internet-based email service - 1989



CompuServe became one of the first ISPs to offer email to their customers before it was taken over by AOL. Photograph: Neal Lauron/Reuters

CompuServe became the first online service to offer internet connectivity via dial-up phone connections, and its proprietary email service allowed other internet users to send emails to each other.

Lotus Notes launched - 1989



Lotus Notes brought joy of email to millions more workers, although it didn't look quite like this in 1989. Photograph: Roger Tooth/The Guardian

The first version Lotus Notes was released in 1989 by Lotus Development Corporation, which was bought by IBM in 1995.

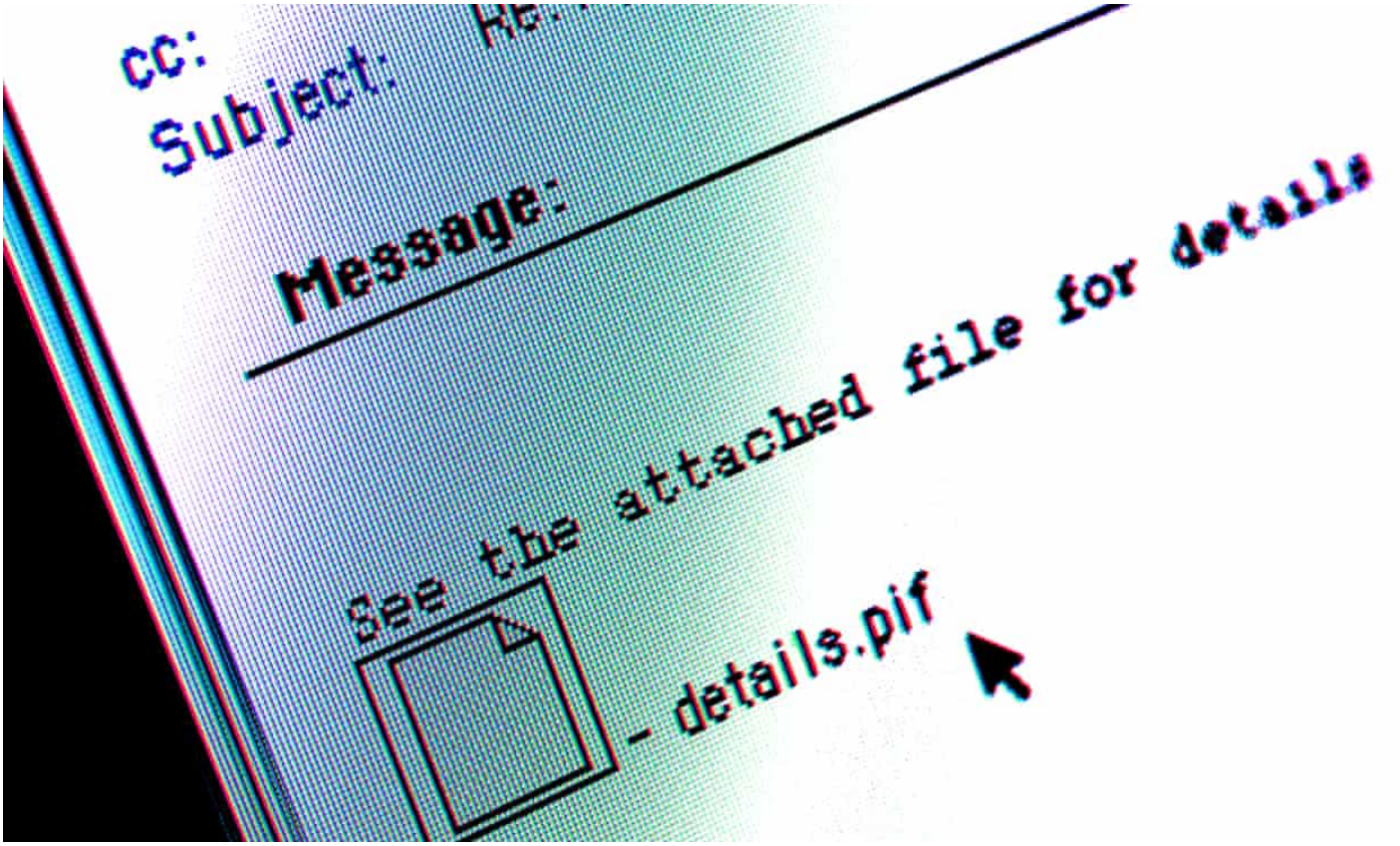
The start of spam - 1990

What's the problem with spam? Photograph: Alamy

The rise of spam can be charted back to the very early days of Arpanet, but it wasn't until the early 1990s that it hit users across the internet, when it was aimed at message boards and later email addresses.

April 1994 is the first recorded business practice of spam from two lawyers from Phoenix, Laurence Carter and Martha Siegel, who ended up writing a book on it.

The attachment - 1992



The attachment was born in 1992, another vector for computer viruses such as the Sobig F to spread
Photograph: Roger Tooth/The Guardian

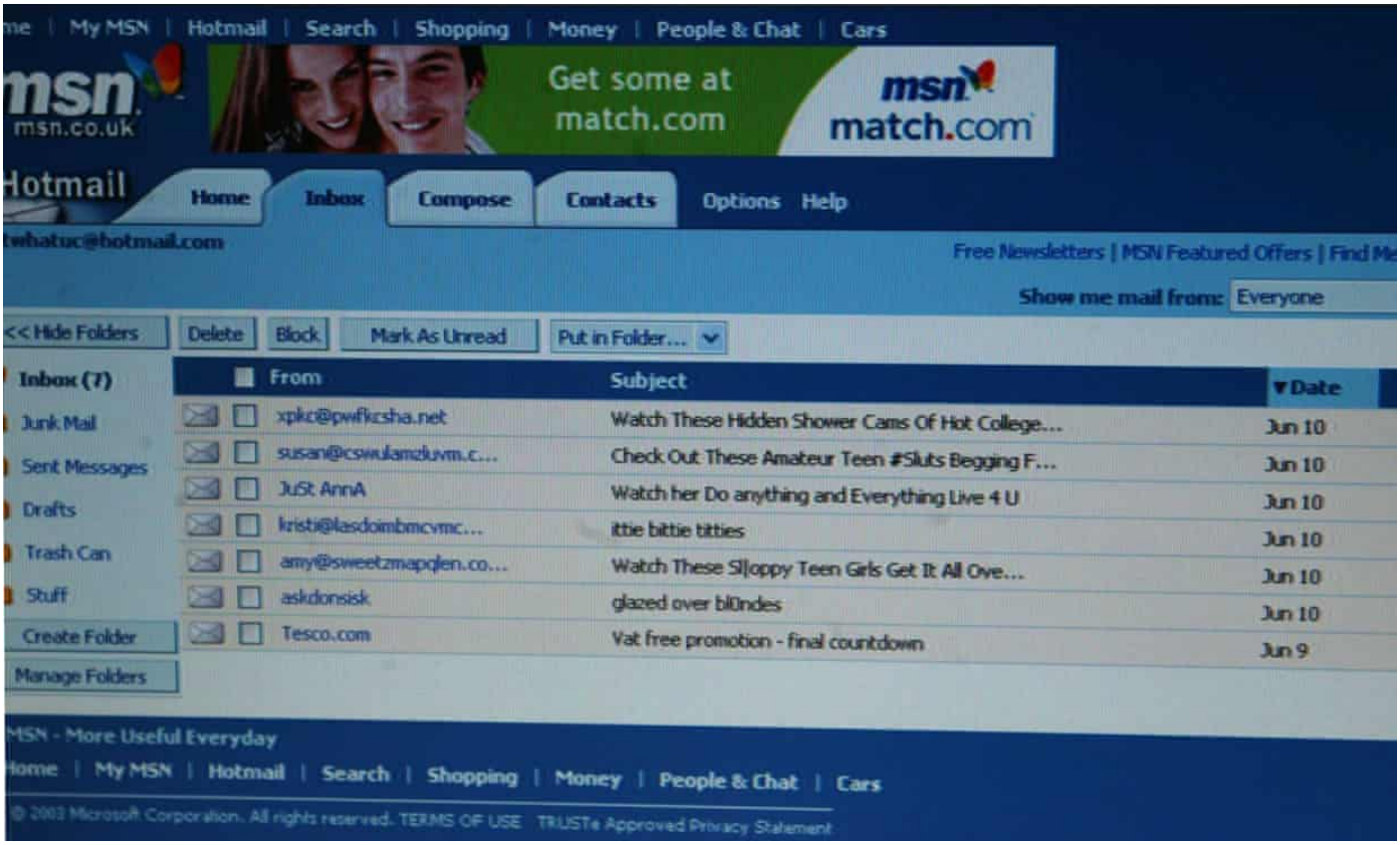
The attachment was born when the Multipurpose Internet Mail Extensions (Mime) protocol was released, which includes the ability to attach things that are not just text to emails. And so begins the painful exercise of trying to delete emails to make space after someone sends you a massive attachment in the days of limited inbox space.

Outlook and Aol - 1993

The iconic AOL CD that cluttered homes for years. Photograph: David Sillitoe/The Guardian

The first version of Microsoft's Outlook was released in 1993 as part of Exchange Server 5.5, while at the same time US internet service providers AOL and Delphi connected their email systems, paving the way for modern, overloaded email systems we struggle with today.

Hotmail launches - 1996

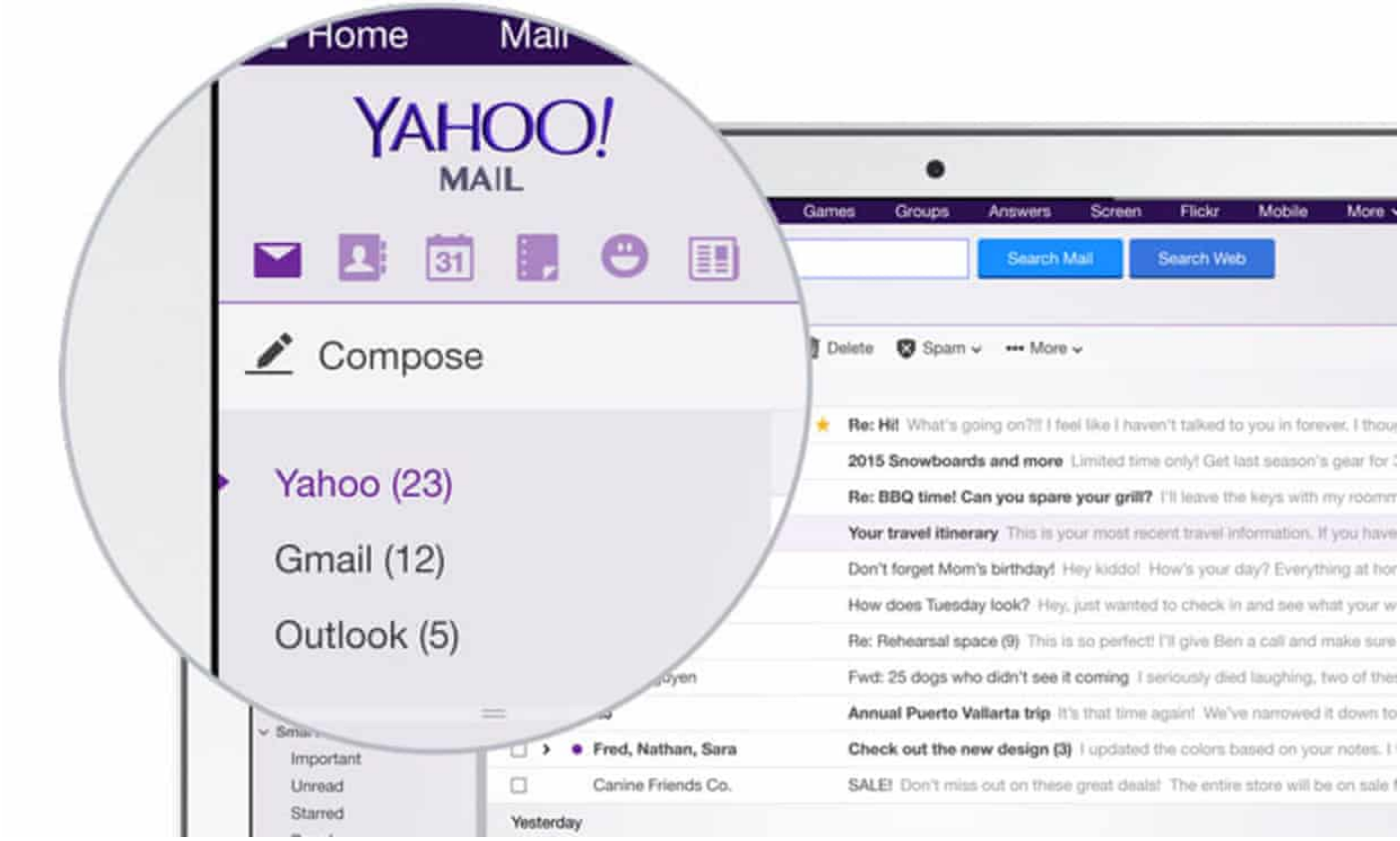


Microsoft's Hotmail was one of the first popular, ISP-agnostic web-based email services. Photograph: Sean Smith/The Guardian

Before Microsoft bought it for $400m, 1996 saw the launch of one of the first popular webmail email services called HoTMaiL developed by Sabeer Bhatia and Jack Smith. It was one of the first email services not tied to a particular ISP and adopted new HTML-based email formatting - hence the stylising of the brand name.

It was bought by Microsoft in 1997, rebranded MSN Hotmail, then Windows Live Hotmail and replaced by Outlook.com in 2013.

Yahoo Mail follows - 1997



Yahoo Mail has been through several revamps in its 9-year history. Photograph: Yahoo

Yahoo Mail was launched the year after Hotmail, which was gaining users by the thousands, and was based on internet company Four11's Rocketmail, which was bought as part of Yahoo's acquisition of the company.

You've Got Mail, and so has everyone else - 1998

Still from the romantic comedy film You've Got Mail, starring Tom Hanks and Meg Ryan. Photograph: Warner Bros

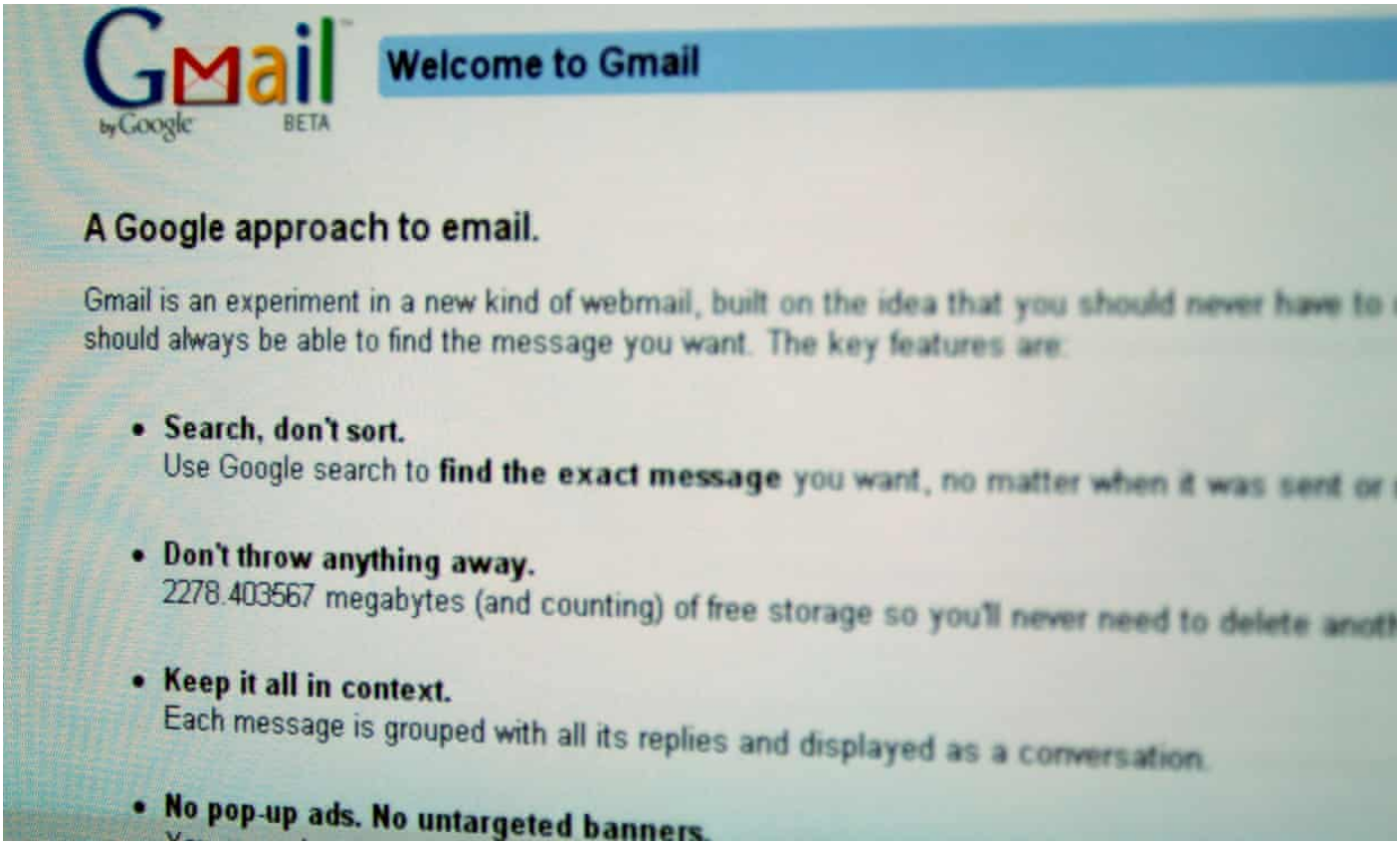
Email was cemented in the public consciousness with the notorious “you’ve got mail” sound of email arriving for AOL users, which formed the cornerstone of the 1998 Tom Hanks and Meg Ryan romantic comedy, You’ve Got Mail.

By the late 1990s spam was becoming a real problem - inducted to the Oxford English Dictionary in 1998 - as more and more marketers jumped on the practically zero-cost outreach proposition and inundated our inboxes.

In 2002, the European Union released its Directive on Privacy and Electronic Communications, which included a section on spam that made it illegal to send unsolicited communications for direct marketing purposes without prior consent of the recipient.

The US passed similar laws in 2004, although neither have been particularly effective at reducing the load.

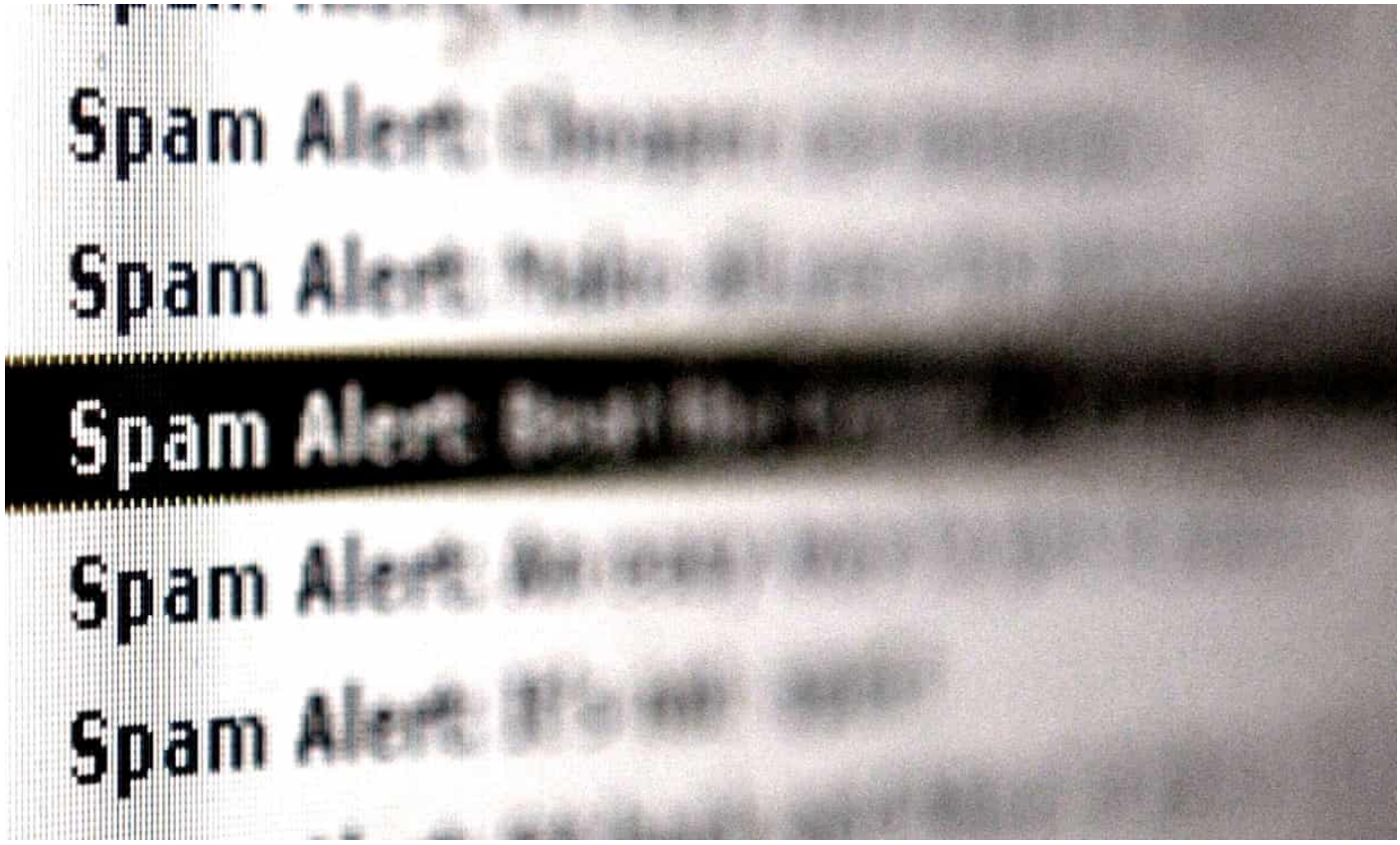
Gmail launches - 2004



Gmail, or Googlemail as it was once known in the olden days. Photograph: Dean Murray / Rex Features

Google's popular email service, Gmail, started life as an internal mail system for Google employees, developed by Paul Buchheit in 2001. It wasn't unveiled to the public until a limited, invite-only beta release in 2004. It was made publicly available in 2007 and dropped its "beta" status in 2009.

Fighting back against spam - 2005



Email protocols started fighting back against spam in the early 2000s. Photograph: Ian Waldie/Getty Images

The first email standard to attempt to fight the deluge of spam by verifying senders was published after a five-year development. Sender Policy Framework was then implemented by a variety of anti-spam programs. A standard of authentication to attempt to prevent email spoofing and phishing was also released called DomainKeys Identified Mail (DKIM).

Email goes mobile for casual users - 2007

Little did Steve Jobs know that the Mail icon on the iPhone would forever show thousands unread. Photograph: Paul Sakuma/AP

Apple's first iPhone was released in 2007, which began to introduce mobile email to the consumer masses. Until that point pre-capacitive consumer smartphones typically had limited email support, while RIM's BlackBerry had brought the burden of work email to employee palms starting in 2003.

Buried in email - 2015

Buried in email. Photograph: LifeStyleKB / Alamy/Alamy

From humble internal communications beginnings, email now dominates a vast proportion of everyday life. An estimated 4.4bn email addresses are in use worldwide with 205bn emails sent per day in 2015, according to data from market research firm Radicati Group.

That number is set to increase to over 246bn emails a day by the end of 2019.

What was the best (and worst) email you ever received?

12 things today's gamers don't remember about old games