CHAPTER 7: OTHER INFORMATION PROPERTY

A. Personal Data

IN RE ESTATE OF SWEZEY
No. 2017-2976/A (N.Y Sur. Ct. N.Y. Co. Jan. 14, 2019)

Mella, Judge: ...

Nicholas Scandalios, in his capacity as executor of the estate of decedent Ric Swezey, petitions for turnover from Apple, Inc. of photographs stored in decedent's iTunes and/or iCloud account ("Apple account").[1] Specifically, petitioner seeks an order directing Apple to disclose this data. According to petitioner, he was informed by Apple that a court order would be required before it discloses "data contained within [an] Apple ID."[2] Apple has not filed a responsive pleading and did not appear on the September 4, 2018 return date of the citation of this proceeding.

Decedent died unexpectedly in 2017, at age 45, survived by petitioner, his spouse, and their two minor children. Under decedent's will admitted to probate on January 26, 2018, decedent left to petitioner all of his personal property, with some exceptions that are irrelevant to the relief sought here, along with the residuary estate. According to petitioner, decedent was an "avid photographer" who took the majority of their family photographs as well as artistic photos using both a digital camera and an iPhone. Petitioner believes that decedent stored his photographs in his Apple account because decedent used his iPhone for many of the family photographs and thus the images were automatically stored there. In addition, petitioner and decedent often viewed the photographs together on decedent's computer and used the Apple system to make holiday photo cards. Petitioner fur-

1. Originally, petitioner sought to "access and obtain control of decedent's personal property stored on [decedent's] computer, iPhone and in the iCloud, and iTunes account under [decedent's] Apple IDs," but, in an affidavit filed on October 1, 2018, he clarified that "the sole purpose" of this application was to "access and obtain control of [petitioner and decedent's] photographs stored in [decedent's] iTunes and/or iCloud account(s)." In light of this, the court finds it unnecessary to address the broader relief originally sought.

2. Attached to the petition is a copy of an email dated November 2, 2017, from Apple's Digital Estate team in response to petitioner's request for access, in which Apple requires a court order making the following findings in order to allow petitioner to change the passwords and access data contained within decedent's Apple ID:

   (1) "The decedent was the user of all accounts associated with the Apple ID";

   (2) "The requestor is the legal personal representative of the decedent";

   (3) "As legal personal representative, the requestor is the 'agent' of the decedent, and their [sic] authorization constitutes `lawful consent' as those terms are used in the Electronic Communications Privacy Act"; and

   (4) "Apple is ordered by the court to assist in the recovery of decedent's personal data from their accounts, which may contain third party personally identifiable information or data, from their accounts."

ther states that decedent had two e-mail accounts which could be the Apple ID associated with the Apple account and identifies those email accounts based on his personal knowledge. Petitioner states that, had decedent not died unexpectedly, he and decedent would have transferred the photographs to petitioner's Apple account as they had intended to.

No provision in decedent's will expressly authorizes the executor to access decedent's digital assets and petitioner points to no other documents authorizing such access. Nor does petitioner provide proof of decedent's use of any online tool granting his personal representative access to his digital property. Nevertheless, petitioner alleges that he and decedent gave to each other implicit consent to access each other's digital assets as evidenced, for instance, by the fact that their computers were adjacent to each other in their home office and there was "never any effort to shield [their] computer screens or [their] access to [their] digital assets from one another."

In this age, a decedent's property—which is defined as "anything that may be the subject of ownership," real or personal (EPTL 1-2.15; *see* SCPA 103 [44]) — must include assets kept in a digital form in cyberspace. The New York legislature enacted Article 13-A of the Estates, Powers and Trusts Law to apply traditional laws governing fiduciaries to this "new type of property" and authorize fiduciaries to "gain access to, manage, distribute and copy or delete digital assets" (Sponsor's Mem, Bill Jacket, L 2016, ch 354). Fiduciaries are now charged with the same duty of care, loyalty, and confidentiality to marshal and protect a decedent's digital assets as they do to manage a decedent's tangibles (EPTL 13-A-4.1 [a]).

Digital assets are "electronic record[s] in which an individual has a right or interest" (EPTL 13-A-1 [i]), which consist of electronic communications and other digital assets that are not electronic communications. This distinction is significant in that disclosure of electronic communications, unlike disclosure of other digital assets, requires proof of a user's consent or a court order.

Here, decedent's photographs stored in his Apple account are not "electronic communications," the disclosure of which, in the absence of a court order, requires consent of the account holder in any form listed under EPTL 13-A-2.2. Therefore, Apple is required to disclose the photographs stored in decedent's Apple account associated with his Apple ID identifiable by decedent's two email accounts as listed in the petition (EPTL 13-A-3.2).

Accordingly, and in order to provide petitioner with the order that he seeks to satisfy Apple's request, the court makes findings and enters directions as follows (EPTL 13-A-3.2 [d][4]): (1) decedent was the user of an account with Apple, the ID for which is either of the two email accounts provided by petitioner, an individual with personal knowledge that decedent was the user of those email accounts; (2) petitioner is the fiduciary of decedent's estate; and (3) no lawful consent is required for disclosure of these photographs under the Stored Communications Act (18 USC §§ 2701 *et seq.* [part of the Electronic Communication Privacy Act of 1986]) or the New York Administration of Digital Assets law (EPTL Article 13-A) and, in fact, EPTL 13-A-3.2 mandates disclosure of such.

Based on these findings, upon service of a copy of this decision and order, Apple shall afford petitioner the opportunity to reset the password to decedent's Apple ID.

NOTES

1. Apple objected, but it didn't object very hard. Why didn't it simply comply with Scandalios's request for access to Swezey's account? And why didn't it

raise an X-style objection, insisting that the account was its property, and never Swezey's? If you understand both halves of Apple's motivation, you understand this case—the court's reasoning is almost beside the point.

2. Notice that the statutory framework treats "electronic communications" differently than other account contents. The reasoning here has to do with the heightened privacy protections provided by anti-wiretapping laws—communications are regarded as categorically more sensitive than other materials.
3. Note the portion of the opinion that begins, "No provision in decedent's will expressly authorizes the executor to access decedent's digital assets ... ." Providing express instructions and authorization for the handling of the decedent's accounts and other digital assets is now a standard part of estate planning.
4. What do you want to happen to your accounts when you die?

CALIFORNIA PRIVACY RIGHTS ACT*

California Civil Code

§ 1798.105 – *Consumers' Right to Delete Personal Information*

(a) A consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer. ...

(d) A business ... shall not be required to comply with a consumer's request to delete the consumer's personal information if it is reasonably necessary for the business, service provider, or contractor to maintain the consumer's personal information in order to:

(1) Complete the transaction for which the personal information was collected, fulfill the terms of a written warranty or product recall conducted in accordance with federal law, provide a good or service requested by the consumer, or reasonably anticipated by the consumer within the context of a business' ongoing business relationship with the consumer, or otherwise perform a contract between the business and the consumer.

(2) Help to ensure security and integrity to the extent the use of the consumer's personal information is reasonably necessary and proportionate for those purposes.

(3) Debug to identify and repair errors that impair existing intended functionality.

(4) Exercise free speech, ensure the right of another consumer to exercise that consumer's right of free speech, or exercise another right provided for by law. ...

(6) Engage in public or peer-reviewed scientific, historical, or statistical research that conforms or adheres to all other applicable ethics and privacy laws, when the business' deletion of the information is likely

---

* The California Consumer Privacy Act (CCPA) was enacted in 2018. The California Privacy Rights Act (CPRA) was enacted in 2020 by ballot initiative and substantially amended the CCPA. California's privacy-law framework is commonly referred to as the CCPA, the CPRA, or both.

to render impossible or seriously impair the ability to complete such research, if the consumer has provided informed consent.

(7) To enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business and compatible with the context in which the consumer provided the information.

(8) Comply with a legal obligation. ...

§ 1798.120 – *Consumers' Right to Opt Out of Sale or Sharing of Personal Information*

(a) A consumer shall have the right, at any time, to direct a business that sells or shares personal information about the consumer to third parties not to sell or share the consumer's personal information. ...

(c) Notwithstanding subdivision (a), a business shall not sell or share the personal information of consumers if the business has actual knowledge that the consumer is less than 16 years of age, unless the consumer, in the case of consumers at least 13 years of age and less than 16 years of age, or the consumer's parent or guardian, in the case of consumers who are less than 13 years of age, has affirmatively authorized the sale or sharing of the consumer's personal information. ...

§ 1798.121 – *Consumers' Right to Limit Use and Disclosure of Sensitive Personal Information*

(a) A consumer shall have the right, at any time, to direct a business that collects sensitive personal information about the consumer to limit its use of the consumer's sensitive personal information to that use which is necessary to perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services ...

§ 1798.125 – *Consumers' Right of No Retaliation Following Opt Out or Exercise of Other Rights*

(a)

(1) A business shall not discriminate against a consumer because the consumer exercised any of the consumer's rights under this title, including, but not limited to, by:

(A) Denying goods or services to the consumer.

(B) Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties.

(C) Providing a different level or quality of goods or services to the consumer.

(D) Suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services.

(E) Retaliating against an employee, applicant for employment, or independent contractor ...

(2) Nothing in this subdivision prohibits a business, pursuant to subdivision (b), from charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the business by the consumer's data.

(3) This subdivision does not prohibit a business from offering loyalty, rewards, premium features, discounts, or club card programs consistent with this title.

(b)

(1) A business may offer financial incentives, including payments to consumers as compensation, for the collection of personal information, the sale or sharing of personal information, or the retention of personal information. ...

§ 1798.135 – *Methods of Limiting Sale, Sharing, and Use of Personal Information and Use of Sensitive Personal Information*

(a) A business that sells or shares consumers' personal information or uses or discloses consumers' sensitive personal information for purposes other than those authorized by subdivision (a) of Section 1798.121 shall, in a form that is reasonably accessible to consumers:

(1) Provide a clear and conspicuous link on the business's internet homepages, titled "Do Not Sell or Share My Personal Information," to an internet web page that enables a consumer, or a person authorized by the consumer, to opt-out of the sale or sharing of the consumer's personal information.

(2) Provide a clear and conspicuous link on the business' internet homepages, titled "Limit the Use of My Sensitive Personal Information," that enables a consumer, or a person authorized by the consumer, to limit the use or disclosure of the consumer's sensitive personal information to those uses authorized by subdivision (a) of Section 1798.121. ...

(d) Nothing in this title shall be construed to require a business to comply with the title by including the required links and text on the homepage that the business makes available to the public generally, if the business maintains a separate and additional homepage that is dedicated to California consumers and that includes the required links and text, and the business takes reasonable steps to ensure that California consumers are directed to the homepage for California consumers and not the homepage made available to the public generally. ...

§ 1798.140 – *Definitions*

For purposes of this title: ...

(d) "Business" means:

(1) A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that collects consumers' personal information ... and that ... determines the purposes and means of the processing of consumers' personal information, that does business in the State of California, and that satisfies one or more of the following thresholds:

(A) As of January 1 of the calendar year, had annual gross revenues in excess of twenty-five million dollars ($25,000,000) in the preceding calendar year, as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185.

(B) Alone or in combination, annually buys, sells, or shares the personal information of 100,000 or more consumers or households.

(C) Derives 50 percent or more of its annual revenues from selling or sharing consumers' personal information. ...

(h) "Consent" means any freely given, specific, informed, and unambiguous indication of the consumer's wishes by which the consumer, or the consumer's legal guardian, a person who has power of attorney, or a person acting as a conservator for the consumer, including by a statement or by a clear affirmative action, signifies agreement to the processing of personal information relating to the consumer for a narrowly defined particular purpose. Acceptance of a general or broad terms of use, or similar document, that contains descriptions of personal information processing along with other, unrelated information, does not constitute consent. Hovering over, muting, pausing, or closing a given piece of content does not constitute consent. Likewise, agreement obtained through use of dark patterns does not constitute consent.

(i) "Consumer" means a natural person who is a California resident ...

(ae) "Sensitive personal information" means:

(1) Personal information that reveals:

(A) A consumer's social security, driver's license, state identification card, or passport number.

(B) A consumer's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account.

(C) A consumer's precise geolocation.

(D) A consumer's racial or ethnic origin, citizenship or immigration status, religious or philosophical beliefs, or union membership.

(E) The contents of a consumer's mail, email, and text messages unless the business is the intended recipient of the communication.

(F) A consumer's genetic data. ...

(3) Sensitive personal information that is "publicly available" ... shall not be considered sensitive personal information or personal information.

§ 1798.145 – *Exemptions*

(a)

(1) The obligations imposed on businesses by this title shall not restrict a business's ability to:

(A) Comply with federal, state, or local laws or comply with a court order or subpoena to provide information. ...

(F) Collect, use, retain, sell, share, or disclose consumers' personal information that is deidentified or aggregate consumer information.

(G) Collect, sell, or share a consumer's personal information if every aspect of that commercial conduct takes place wholly outside of California. ...

(2)

(A) This subdivision shall not apply if the consumer's personal information contains information related to accessing, procuring, or searching for services regarding contraception, pregnancy care, and perinatal care, including, but not limited to, abortion services. ...

§ 1798.192 – *Waiver*

Any provision of a contract or agreement of any kind, including a representative action waiver, that purports to waive or limit in any way rights under this title ... shall be deemed contrary to public policy and shall be void and unenforceable. ...

§ 1798.199.10.

(a) There is hereby established in state government the California Privacy Protection Agency, which is vested with full administrative power, authority, and jurisdiction to implement and enforce the California Consumer Privacy Act of 2018. ...

§ 1798.199.55.

(a) When the agency determines there is probable cause for believing this title has been violated, it shall hold a hearing to determine if a violation has or violations have occurred. ... If the agency determines on the basis of the hearing conducted pursuant to this subdivision that a violation or violations have occurred, it shall issue an order that may require the violator to do all or any of the following:

(1) Cease and desist violation of this title.

(2) Subject to Section 1798.155, pay an administrative fine of up to two thousand five hundred dollars ($2,500) for each violation, or up to seven thousand five hundred dollars ($7,500) for each intentional violation and each violation involving the personal information of minor consumers ...

QUESTIONS

1. Does the CPRA create a form of property in personal data?

E.U. GENERAL DATA PROTECTION REGULATION

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC
[2016] OJ L 119/1

art. 1 – *Subject-matter and objectives*

(1) This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.

(2) This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data. ...

art. 2 – ***Material scope***

(1) This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

(2) This Regulation does not apply to the processing of personal data: ...

(c) by a natural person in the course of a purely personal or household activity;

(d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. ...

art. 3 – ***Territorial scope***

(1) This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

(2) This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

(b) the monitoring of their behaviour as far as their behaviour takes place within the Union. ...

art. 4 –***Definitions***

For the purposes of this Regulation:

(1) personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

(2) 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction; ...

(7) 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

(8) 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller; ...

(11) 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a

statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her; ...

art. 5 – *Principles relating to processing of personal data*

(1) Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) ... ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

(2) The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

art. 6 – *Lawfulness of processing*

(1) Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

art. 7 – ***Conditions for consent***

(1) Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

(2) If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. …

(3) The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

art. 9 – ***Processing of special categories of personal data***

(1) Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

(2) Paragraph 1 shall not apply if one of the following applies:

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject; …

(e) processing relates to personal data which are manifestly made public by the data subject; …

(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject; …

art. 13 – ***Information to be provided where personal data are collected from the data subject***

(1) Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

(a) the identity and the contact details of the controller and, where applicable, of the controller's representative; …

(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; …

(2) In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject

with the following further information necessary to ensure fair and transparent processing:

(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

(b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;

(c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(d) the right to lodge a complaint with a supervisory authority;

(e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

(f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

(3) Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

art. 15 – Right of access by the data subject

(1) The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

[information analogous to categories quoted above in art. 13 and also]

(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations; ...

(g) where the personal data are not collected from the data subject, any available information as to their source; ...

(3) The controller shall provide a copy of the personal data undergoing processing. ... Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

(4) The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.

art. 16 – *Right to rectification*

The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. ...

art. 17 – *Right to erasure ('right to be forgotten')*

(1) The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;

(c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);

(d) the personal data have been unlawfully processed; ...

(2) Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

(3) Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

(a) for exercising the right of freedom of expression and information;

(b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(c) for reasons of public interest in the area of public health ...

(d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

(e) for the establishment, exercise or defence of legal claims.

art. 20 – *Right to data portability*

(1) The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

(a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and

(b) the processing is carried out by automated means.

(2) In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible. ...s

art. 21 – *Right to object*

(1) The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims. ...

(3) Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes. ...

art. 28 – *Processor*

(1) Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject. ...

(3) Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. ...

art. 51 – *Supervisory authority*

(1) Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ('supervisory authority'). ...

art 77 – *Right to lodge a complaint with a supervisory authority*

(1) Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation. ...

art. 82 – *Right to compensation and liability*

(1) Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.

art. 85 – *Processing and freedom of expression and information*

(1) Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression.

(2) For processing carried out for journalistic purposes or the purpose of academic artistic or literary expression, Member States shall provide for exemptions or derogations from [most of the provisions of the GDPR] if they are

necessary to reconcile the right to the protection of personal data with the freedom of expression and information.

NOTES

1. The GDPR is law only in the European Union. Nonetheless, it has been influential worldwide (including in some states in the United States), and some companies apply GDPR protections globally. The usual name for this influence is the "Brussels effect."
2. Does the GDPR create a form of property in personal data?

E.U. DATA ACT

Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data … 2023 (O.J. L. 2854)

art. 3 – ***Obligation to make product data and related service data accessible to the user***

1. Connected products shall be designed and manufactured, and related services shall be designed and provided, in such a manner that product data and related service data, including the relevant metadata necessary to interpret and use those data, are, by default, easily, securely, free of charge, in a comprehensive, structured, commonly used and machine-readable format, and, where relevant and technically feasible, directly accessible to the user. …

art. 4 – ***The rights and obligations of users and data holders with regard to access, use and making available product data and related service data***

1. Where data cannot be directly accessed by the user from the connected product or related service, data holders shall make readily available data, as well as the relevant metadata necessary to interpret and use those data, accessible to the user without undue delay, of the same quality as is available to the data holder, easily, securely, free of charge, in a comprehensive, structured, commonly used and machine-readable format and, where relevant and technically feasible, continuously and in real-time. This shall be done on the basis of a simple request through electronic means where technically feasible.
2. Users and data holders may contractually restrict or prohibit accessing, using or further sharing data, if such processing could undermine security requirements of the connected product, as laid down by Union or national law, resulting in a serious adverse effect on the health, safety or security of natural persons. …
4. Data holders shall not make the exercise of choices or rights under this Article by the user unduly difficult, including by offering choices to the user in a non-neutral manner or by subverting or impairing the autonomy, decision-making or choices of the user via the structure, design, function or manner of operation of a user digital interface or a part thereof.
5. For the purpose of verifying whether a natural or legal person qualifies as a user for the purposes of paragraph 1, a data holder shall not require that person to provide any information beyond what is necessary. Data holders shall not keep any information, in particular log data, on the user's access to the data requested beyond what is necessary for the sound execution of the

user's access request and for the security and maintenance of the data infrastructure. ...

art. 5 – *Right of the user to share data with third parties*

1. Upon request by a user, or by a party acting on behalf of a user, the data holder shall make available readily available data, as well as the relevant metadata necessary to interpret and use those data, to a third party without undue delay, of the same quality as is available to the data holder, easily, securely, free of charge to the user, in a comprehensive, structured, commonly used and machine-readable format and, where relevant and technically feasible, continuously and in real-time. The data shall be made available by the data holder to the third party in accordance with Articles 8 and 9.

art. 8 – *Conditions under which data holders make data available to data recipients*

1. Where, in business-to-business relations, a data holder is obliged to make data available to a data recipient under Article 5 or under other applicable Union law or national legislation adopted in accordance with Union law, it shall agree with a data recipient the arrangements for making the data available and shall do so under fair, reasonable and non-discriminatory terms and conditions and in a transparent manner ...

art. 9 – *Compensation for making data available*

1. Any compensation agreed upon between a data holder and a data recipient for making data available in business-to-business relations shall be non-discriminatory and reasonable and may include a margin. ...

art. 11 – *Technical protection measures on the unauthorised use or disclosure of data*

1. A data holder may apply appropriate technical protection measures, including smart contracts and encryption, to prevent unauthorised access to data, including metadata, and to ensure compliance with Articles 4, 5, 6, 8 and 9, as well as with the agreed contractual terms for making data available. Such technical protection measures shall not discriminate between data recipients or hinder a user's right to obtain a copy of, retrieve, use or access data, to provide data to third parties pursuant to Article 5 or any right of a third party under Union law or national legislation adopted in accordance with Union law. Users, third parties and data recipients shall not alter or remove such technical protection measures unless agreed by the data holder. ...

NOTES

1. Does the E.U. Data Act create a form of property in personal data?

B. Trade Secret

UNIFORM TRADE SECRETS ACT

§ 1 – *Definitions*

As used in this [Act], unless the context requires otherwise:

(1) "Improper means" includes theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means;

(2) "Misappropriation" means:

(i) acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means; or

(ii) disclosure or use of a trade secret of another without express or implied consent by a person who

(A) used improper means to acquire knowledge of the trade secret; or

(B) at the time of disclosure or use, knew or had reason to know that his knowledge of the trade secret was

(I) derived from or through a person who had utilized improper means to acquire it;

(II) acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use; or

(III) derived from or through a person who owed a duty to the person seeking relief to maintain its secrecy or limit its use; or

(C) before a material change of his [or her] position, knew or had reason to know that it was a trade secret and that knowledge of it had been acquired by accident or mistake. ...

(4) "Trade secret" means information, including a formula, pattern, compilation, program, device, method, technique, or process, that:

(i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and

(ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

Comment

One of the broadly stated policies behind trade secret law is "the maintenance of standards of commercial ethics." *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470 (1974). The Restatement of Torts, Section 757, Comment (f), notes: "A complete catalogue of improper means is not possible," but Section 1(1) includes a partial listing.

Proper means include:

1. Discovery by independent invention;
2. Discovery by "reverse engineering", that is, by starting with the known product and working backward to find the method by which it was developed. The acquisition of the known product must, of course, also be by a fair and honest means, such as purchase of the item on the open market for reverse engineering to be lawful;
3. Discovery under a license from the owner of the trade secret;
4. Observation of the item in public use or on public display;
5. Obtaining the trade secret from published literature.

Improper means could include otherwise lawful conduct which is improper under the circumstances; *e.g.,* an airplane overflight used as aerial reconnaissance to de-

termine the competitor's plant layout during construction of the plant. *E. I. du Pont de Nemours & Co., Inc. v. Christopher*, 431 F.2d 1012 (CA5, 1970), cert. den. 400 U.S. 1024 (1970). Because the trade secret can be destroyed through public knowledge, the unauthorized disclosure of a trade secret is also a misappropriation.

The type of accident or mistake that can result in a misappropriation under Section 1(2)(ii)(C) involves conduct by a person seeking relief that does not constitute a failure of efforts that are reasonable under the circumstances to maintain its secrecy under Section 1(4)(ii).

The definition of "trade secret" contains a reasonable departure from the Restatement of Torts (First) definition which required that a trade secret be "continuously used in one's business." The broader definition in the proposed Act extends protection to a plaintiff who has not yet had an opportunity or acquired the means to put a trade secret to use. The definition includes information that has commercial value from a negative viewpoint, for example the results of lengthy and expensive research which proves that a certain process will *not* work could be of great value to a competitor. *Cf. Telex Corp. v. IBM Corp.,* 510 F.2d 894 (10th Cir. 1975) (liability imposed for developmental cost savings with respect to product not marketed). Because a trade secret need not be exclusive to confer a competitive advantage, different independent developers can acquire rights in the same trade secret.

The words "method, technique" are intended to include the concept of "know-how."

The language "not being generally known to and not being readily ascertainable by proper means by other persons" does not require that information be generally known to the public for trade secret rights to be lost. If the principal person persons who can obtain economic benefit from information is are aware of it, there is no trade secret. A method of casting metal, for example, may be unknown to the general public but readily known within the foundry industry.

Information is readily ascertainable if it is available in trade journals, reference books, or published materials. Often, the nature of a product lends itself to being readily copied as soon as it is available on the market. On the other hand, if reverse engineering is lengthy and expensive, a person who discovers the trade secret through reverse engineering can have a trade secret in the information obtained from reverse engineering.

Finally, reasonable efforts to maintain secrecy have been held to include advising employees of the existence of a trade secret, limiting access to a trade secret on "need to know basis", and controlling plant access. On the other hand, public disclosure of information through display, trade journal publications, advertising, or other carelessness can preclude protection.

The efforts required to maintain secrecy are those "reasonable under the circumstances." The courts do not require that extreme and unduly expensive procedures be taken to protect trade secrets against flagrant industrial espionage. It follows that reasonable use of a trade secret including controlled disclosure to employees and licensees is consistent with the requirement of relative secrecy.

NOTES

1. The UTSA is a model statute; it has been enacted in some form in forty-eight states and the District of Columbia. The text of state enactments varies, as do judicial interpretations. The UTSA is state law; the federal Defend Trade Secrets Act (DTSA), Pub. L. No. 114–153, 130 Stat. 376 (2016), 18 U.S.C. § 1836 *et. seq.*, adopts many of the UTSA's definitions in creating a federal

civil cause of action for trade-secret misappropriation. The federal Economic Espionage Act (EEA), Pub. L. No. 104–294, 110 Stat. 3488 (1996), 18 U.S.C. § 1831 *et seq.*, provides criminal penalties for some trade-secret thefts, as do some state statutes like the New York one discussed below in *Aleynikov II*.

RELIGIOUS TECHNOLOGY CENTER V. LERMA

908 F. Supp. 1362 (E.D. Va. 1995)

Brinkema, District Judge: ...

1. Undisputed Facts

The essential facts are not in dispute. In 1991, the Church of Scientology sued Steven Fishman, a disgruntled former member of the Church of Scientology, in the United States District Court for the Central District of California. On April 14, 1993, Fishman filed in the open court file what has come to be known as the Fishman affidavit, to which were attached 69 pages of what the Religious Technology Center describes as various Advanced Technology works, specifically levels OT-I through OT-VII documents. Plaintiff claims that these documents are protected from both unauthorized use and unauthorized disclosure under the copyright laws of the United States and under trade secret laws, respectively.

In California, the RTC moved to seal the Fishman affidavit, arguing that the attached AT documents were trade secrets. That motion was denied and the Ninth Circuit upheld the district court's decision not to seal the file. The case was remanded for further proceedings and the district court again declined to seal the file, which remained unsealed until August 15, 1995.

Defendant Arnaldo Lerma, another former Scientologist, obtained a copy of the Fishman affidavit and the attached AT documents. Lerma admits that on July 31 and August 1, 1995, he published the AT documents on the Internet through defendant Digital Gateway Systems, an Internet access provider. RTC, which regularly scans the Internet, discovered the publication of documents and on August 11, 1995, warned Lerma to return the AT documents and not publish them any further. After Lerma refused to cooperate, RTC obtained a Temporary Restraining Order prohibiting Lerma from any further publication of the documents and a seizure warrant which authorized the United States Marshal to seize Lerma's personal computer, floppy disks and any copies of the copyrighted works of L. Ron Hubbard, the author of the AT documents.

During the same time period, on or about August 5 or 6, 1995, Lerma sent a hard copy of the Fishman affidavit and AT attachments to Richard Leiby, an investigative reporter for The Washington Post. On August 12, 1995, counsel for RTC discovered this disclosure and approached The Post, which was told that the Fishman affidavit might be stolen. In response to the RTC's representations, The Post returned the actual copy which Lerma had given it. However, The Post had by then learned that a copy of the same Fishman affidavit was available in the open court file in the United States District Court for the Central District of California. On August 14, 1995, The Post sent Kathryn Wexler, a news aide stationed in California, to that court to obtain a copy of the Fishman affidavit. The Clerk's office made a copy for Wexler, who then mailed it to Washington. Although it is undisputed that RTC staff members had been checking that file out and holding it all day to prevent anyone from seeing it, the file was not sealed and obviously was available, upon request, to any member of the public who wished to see it.

The day after The Post obtained its copy of the Fishman affidavit, the RTC applied for a sealing order and the trial judge ordered the file sealed. However, there

is no evidence in the record that the judge ordered The Post to return the copy made by the Clerk's office or that any kind of a restraining order was issued by that court against The Post.

Five days later, on August 19, 1995, The Post published a news article, entitled "Church in Cyberspace: Its Sacred Writ is on the Net. Its Lawyers are on the Case," written by defendant Marc Fisher. In that article, RTC's lawsuit against Lerma and the seizure of his computer equipment were discussed, as was the history of Scientology litigation against its critics and the growing use of the Internet by Scientology dissidents. The article included three brief quotes (totalling 46 words) from three of the AT documents. On August 22, 1995, the RTC filed its First Amended Verified Complaint for Injunctive Relief and Damages in which it added The Washington Post and its two reporters, Fisher and Leiby, as additional defendants. A Second Amended Verified was later filed and is now the subject of this summary judgment motion. ...

II. THE COPYRIGHT CLAIM

[The court assumed that the AT documents were validly copyrighted, but held that the Post's publication of short excerpts from them were fair use.]

IV. MISAPPROPRIATION CLAIM

To prove misappropriation of a trade secret, the RTC must show (1) that it possessed a valid trade secret, (2) that the defendant acquired its trade secret, and (3) that the defendant knew or should have known that the trade secret was acquired by improper means.

The Post argues persuasively that the AT documents were no longer trade secrets by the time The Post acquired them. They point to the following undisputed facts. First, the Fishman affidavit had been in a public court file from April 14, 1993 until August 15, 1995, for a total of 28 months. Although RTC has shown that it went to extraordinary efforts to control access to that file by having church members sign out the file and keep it in their custody at the courthouse, the file nevertheless was an open file, available to the public. The Post was able to obtain a copy of the Fishman affidavit without any difficulty, by merely asking the Clerk of the court to copy it. Thus, having been in the public domain for an extensive period of time, these AT documents cannot be deemed trade secrets.

Of even more significance is the undisputed fact that these documents were posted on the Internet on July 31 and August 1, 1995. On August 11, 1995, this Court entered a Temporary Restraining Order among other orders which directed Lerma to stop disseminating the AT documents. However, that was more than ten days after the documents were posted on the Internet, where they remained potentially available to the millions of Internet users around the world.

As other courts who have dealt with similar issues have observed, posting works to the Internet makes them generally known at least to the relevant people interested in the news group. Once a trade secret is posted on the Internet, it is effectively part of the public domain, impossible to retrieve. Although the person who originally posted a trade secret on the Internet may be liable for trade secret misappropriation, the party who merely down loads Internet information cannot be liable for misappropriation because there is no misconduct involved in interacting with the Internet.

Even if one were to assume that the AT documents are still trade secrets, under Virginia law, the tort of misappropriation of trade secrets is not committed by a

person who uses or publishes a trade secret unless that person has used unlawful means, or breached some duty created by contract or implied by law resulting from some employment or similar relationship.

> It is the *employment of improper means to procure the trade secret, rather than the mere copying or use,* which is the basis of [liability] ... Apart from breach of contract, abuse of confidence or impropriety in the means of procurement, trade secrets may be copied freely as devices or processes which are not secret.

Trandes Corporation v. Guy F. Atkinson Company, 996 F.2d 656, 660 (4th Cir. 1993) (quoting the Restatement (First of Torts)) (emphasis in original). The *Trandes* court notes that abuse of confidence or impropriety in the means of procurement represented the "essential element" and the "core" of a misappropriation claim. *Id.*

The RTC claims that because The Post was on notice of the RTC's allegations that the AT documents were stolen and were both trade secrets and unpublished copyrighted works, The Post was under a legal obligation not to copy or use the documents. This Court knows of no law which required The Post to sit on its hands and do no further investigation into what was obviously becoming a newsworthy event and newsworthy documents. The RTC's allegations are still just allegations. The very court from which the Fishman affidavit was obtained still has under advisement the issue of whether the AT documents are trade secrets. Although The Post was on notice that the RTC made certain proprietary claims about these documents, there was nothing illegal or unethical about The Post going to the Clerk's office for a copy of the documents or downloading them from the Internet.

Because there is no evidence that The Post abused any confidence, committed an impropriety, violated any court order or committed any other improper act in gathering information from the court file or down loading information from the Internet, there is no possible liability for The Post in its acquisition of the information. This is true regardless of the documents' status as trade secrets. As for the disclosure of the information, The Post did nothing more than briefly quote from publicly available materials. These acts simply do not approach a trade secret misappropriation, and, therefore, summary judgment must be entered for the defendants. ...

NOTES

1. *Lerma* illustrates a crucial difference between copyright and trade secret—and a crucial weakness of trade secret, from a plaintiff's perspective. Copyright applies against anyone who reproduces the work without permission, but trade secret is limited by the definition of misappropriation. A trade secret claim lies only against a defendant who breaches a confidence or uses improper means to obtain the information, or knows or has reason to know that they are downstream of someone who did. Indeed, if the information becomes widely enough available—even as a result of misappropriation—it ceases to be a trade secret at all, and can be freely used by anyone.
2. Why did the Post both (a) send an employee to the courthouse to obtain a copy of the AT documents, and (b) return the copy of the AT documents it received from Lerma?

UNITED STATES V. ALEYNIKOV [ALEYNIKOV I]

676 F.3d 71 (2nd Cir. 2012)

Jacobs, Chief Judge:

Sergey Aleynikov was convicted, following a jury trial in the United States District Court for the Southern District of New York of stealing and transferring some of the proprietary computer source code used in his employer's high frequency trading system, in violation of the National Stolen Property Act, 18 U.S.C. § 2314 (the "NSPA") and the Economic Espionage Act of 1996, 18 U.S.C. § 1832 (the "EEA"). [The EEA portions of the opinion are omitted.]

Background

Sergey Aleynikov, a computer programmer, was employed by Goldman Sachs & Co. ("Goldman") from May 2007 through June 2009, developing computer source code for the company's proprietary high-frequency trading ("HFT") system. An HFT system is a mechanism for making large volumes of trades in securities and commodities based on trading decisions effected in fractions of a second. Trades are executed on the basis of algorithms that incorporate rapid market developments and data from past trades. ... High frequency trading is a competitive business that depends in large part on the speed with which information can be processed to seize fleeting market opportunities. Goldman closely guards the secrecy of each component of the system, and does not license the system to anyone. Goldman's confidentiality policies bound Aleynikov to keep in strict confidence all the firm's proprietary information, including any intellectual property created by Aleynikov. He was barred as well from taking it or using it when his employment ended.

By 2009, Aleynikov was earning $400,000, the highest-paid of the twenty-five programmers in his group. In April 2009, he accepted an offer to become an Executive Vice President at Teza Technologies LLC, a Chicago-based startup that was looking to develop its own HFT system. Aleynikov was hired, at over $1 million a year, to develop the market connectivity and infrastructure components of Teza's HFT system. ...

Aleynikov's last day at Goldman was June 5, 2009. At approximately 5:20 p.m., just before his going-away party, Aleynikov encrypted and uploaded to a server in Germany more than 500,000 lines of source code for Goldman's HFT system, including code for a substantial part of the infrastructure, and some of the algorithms and market data connectivity programs. Some of the code pertained to programs that could operate independently of the rest of the Goldman system and could be integrated into a competitor's system. After uploading the source code, Aleynikov deleted the encryption program as well as the history of his computer commands. When he returned to his home in New Jersey, Aleynikov downloaded the source code from the server in Germany to his home computer, and copied some of the files to other computer devices he owned.

On July 2, 2009, Aleynikov flew from New Jersey to Chicago to attend meetings at Teza. He brought with him a flash drive and a laptop containing portions of the Goldman source code. When Aleynikov flew back the following day, he was arrested by the FBI at Newark Liberty International Airport. ...

Discussion

On appeal ... Aleynikov argues that the source code—as purely intangible property—is not a "good" that was "stolen" within the meaning of the NSPA. ...

I

The NSPA makes it a crime to "transport[ ], transmit[ ], or transfer[ ] in interstate or foreign commerce any goods, wares, merchandise, securities or money, of the value of $5,000 or more, knowing the same to have been stolen, converted or taken by fraud." 18 U.S.C. § 2314. ... The decisive question is whether the source code that Aleynikov uploaded to a server in Germany, then downloaded to his computer devices in New Jersey, and later transferred to Illinois, constituted stolen "goods," "wares," or "merchandise" within the meaning of the NSPA. Based on the substantial weight of the case law, as well as the ordinary meaning of the words, we conclude that it did not.

A.

We first considered the applicability of the NSPA to the theft of intellectual property in *United States v. Bottone*, 365 F.2d 389 (2d Cir. 1966) (Friendly, J.), in which photocopied documents outlining manufacturing procedures for certain pharmaceuticals were transported across state lines. Since the actual processes themselves (as opposed to photocopies) were never transported across state lines, the "serious question" (we explained) was whether "the papers showing [the] processes that were transported in interstate or foreign commerce were 'goods' which had been 'stolen, converted or taken by fraud' in view of the lack of proof that any of the physical materials so transported came from [the manufacturer's] possession." *Id.* at 393. We held that the NSPA was violated there, observing that what was "stolen and transported" was, ultimately, "tangible goods," notwithstanding the "clever intermediate transcription [and] use of a photocopy machine." *Id.* However, we suggested that a different result would obtain if there was no physical taking of tangible property whatsoever: "To be sure, where no tangible objects were ever taken or transported, a court would be hard pressed to conclude that 'goods' had been stolen and transported within the meaning of 2314." *Id.* Hence, we observed, "the statute would presumably not extend to the case where a carefully guarded secret formula was memorized, carried away in the recesses of a thievish mind and placed in writing only after a boundary had been crossed." *Id. Bottone* itself thus treats its holding as the furthest limit of a statute that is not endlessly elastic: Some tangible property must be taken from the owner for there to be deemed a "good" that is "stolen" for purposes of the NSPA.

Bottone's reading of the NSPA is confirmed by the Supreme Court's opinion in *Dowling v. United States,* 473 U.S. 207 (1985), which held that the NSPA did not apply to an interstate bootleg record operation. *Dowling* rejected the Government's argument that the unauthorized use of the musical compositions rendered them "stolen, converted or taken by fraud." Cases prosecuted under the NSPA "have always involved physical 'goods, wares, [or] merchandise' that have themselves been 'stolen, converted or taken by fraud'"—even if the stolen thing does not "remain in entirely unaltered form," and "owes a major portion of its value to an intangible component." *Id.* at 216. ...

We join other circuits in relying on *Dowling* for the proposition that the theft and subsequent interstate transmission of purely intangible property is beyond the scope of the NSPA.

In a close analog to the present case, the Tenth Circuit affirmed the dismissal of an indictment alleging that the defendant transported in interstate commerce a computer program containing source code that was taken from his employer. *United States v. Brown*, 925 F.2d 1301, 1305, 1309 (10th Cir. 1991). Citing *Dowling,* the court held that the NSPA "applies only to physical 'goods, wares or mer-

chandise'" and that "[p]urely intellectual property is not within this category. It can be represented physically, such as through writing on a page, but the underlying, intellectual property itself, remains intangible." *Id.* at 1307. The Court concluded that "the computer program itself is an intangible intellectual property, and as such, it alone cannot constitute goods, wares, merchandise, securities or moneys which have been stolen, converted or taken" for purposes of the NSPA. *Id.* at 1308. ...

B.

By uploading Goldman's proprietary source code to a computer server in Germany, Aleynikov stole purely intangible property embodied in a purely intangible format. There was no allegation that he physically seized anything tangible from Goldman, such as a compact disc or thumb drive containing source code, so we need not decide whether that would suffice as a physical theft. Aleynikov later transported portions of the source code to Chicago, on his laptop and flash drive. However, there is no violation of the statute unless the good is transported with knowledge that "the same" has been stolen; the statute therefore presupposes that the thing stolen was a good or ware, etc., *at the time of the theft.* The wording "contemplate[s] a physical identity between the items unlawfully obtained and those eventually transported." *Dowling*, 473 U.S. at 216. The later storage of intangible property on a tangible medium does not transform the intangible property into a stolen good.

The infringement of copyright in *Dowling* parallels Aleynikov's theft of computer code. Although "[t]he infringer invades a statutorily defined province guaranteed to the copyright holder alone[,] . . . he does not assume physical control over the copyright; nor does he wholly deprive its owner of its use." *Id. at 217.* Because Aleynikov did not "assume physical control" over anything when he took the source code, and because he did not thereby "deprive [Goldman] of its use," Aleynikov did not violate the NSPA.

As the district court observed, Goldman's source code is highly valuable, and there is no doubt that in virtually every case involving proprietary computer code worth stealing, the value of the intangible code will vastly exceed the value of any physical item on which it might be stored. But federal crimes are "solely creatures of statute." *Dowling,* 473 U.S. at 213. We decline to stretch or update statutory words of plain and ordinary meaning in order to better accommodate the digital age. ...

PEOPLE V. ALEYNIKOV
[ALEYNIKOV II]
104 N.E.3d 687 (N.Y. 2018)

Fahey, Justice:

Ideas begin in the mind. By its very nature, an idea, be it a symphony or computer source code, begins as intangible property. However, the medium upon which an idea is stored is generally physical, whether it is represented on a computer hard drive, vinyl record, or compact disc. The changes made to a hard drive or disc when information is copied onto it are physical in nature. The representation occupies space. Consequently, a statute that criminalizes the making of a tangible reproduction or representation of secret scientific material by electronically copying or recording applies to the acts of a defendant who uploads proprietary source code to a computer server. ...

[The court described the history of Aleynikov's federal prosecution, which concluded with *Aleynikov I*, above.] In September 2012, defendant was charged in state court with two counts of unlawful use of secret scientific material ... , a class E felony. An individual is guilty of the crime "when, with intent to appropriate . . . the use of secret scientific material, and having no right to do so and no reasonable ground to believe that he [or she] has such right, [the individual] makes a tangible reproduction or representation of such secret scientific material by means of writing, photographing, drawing, mechanically or electronically reproducing or recording such secret scientific material" (Penal Law § 165.07). ...

I.

Defendant's initial contention is that there is legally insufficient evidence that the source code he uploaded and downloaded was tangible within the meaning of Penal Law § 165.07 .

Penal Law § 165.07 , enacted in 1967, was intended to ensure that a defendant who makes a copy of secret scientific material, but does not take the original, is subject to criminal sanction even though the defendant has not committed larceny. ...

The stimulus for the legislation was a federal case, *United States v Bottone*, in which defendants took, photocopied (at home), and then returned secret scientific documents — instructions for the manufacture of antibiotics and a steroid — from a drug manufacturing company, but did not take the documents permanently.The issue in *Bottone* was whether the documents had been "stolen" and "transport[ed]" within the meaning of the federal statute under which the defendants (and much later Aleynikov) were prosecuted, the National Stolen Property Act, 18 U.S.C § 2314. Although the Second Circuit ruled that 18 U.S.C. § 2314 did apply, our legislature acted to ensure that there was no possible gap in the Revised Penal Law of 1967. The legislature thus sought to criminalize misappropriations of intellectual property that were not traditional takings, but resulted in tangible reproductions of the protected material. ...

Without leaving the confines of the trial evidence before us, we conclude that viewing the facts in the light most favorable to the People, a rational jury could have found that the "reproduction or representation" that defendant made of Goldman's source code, when he uploaded it to the German server, was tangible in the sense of "material" or "having physical form." The jury heard testimony that the representation of source code has physical form. Kumar, the computer engineer, testified that while source code, as abstract intellectual property, does not have physical form, the "[r]epresentation of it" is material. He explained that when computer files are stored on a hard drive or CD, they are physically present on that hard drive or disc, and further stated that data is visible "in aggregate" when stored on such a medium. The jury also heard testimony that source code that is stored on a computer "takes up physical space in a computer hard drive." Given that a reproduction of computer code takes up space on a drive, it is clear that it is physical in nature. In short, the changes that are made to the hard drive or disc, when code or other information is stored, are physical.

Defendant contends that if "tangible" means "having physical form," then the statutory term "tangible reproduction" would involve a redundancy because all computer data is stored in some physical medium. We disagree. Someone with a photographic memory who memorized a piece of source code would not be making a tangible reproduction of the code. ...

We conclude that there is legally sufficient evidence that defendant created a tangible copy of the source code on the German server in violation of Penal Law § 165.07. ...

QUESTIONS

1. Although *Aleynikov I* and *Aleynikov II* may seem to be contradictory, they can be reconciled. The federal NSPA is a *stolen property* statute. The judicially added "tangible property" threshold is there because otherwise garden-variety copyright infringement would also be an NSPA violation. But New York's Penal Law § 165.07 is a *trade secret* statute. The statutory "tangible" threshold is there to keep the statute from applying to people who memorize confidential information.
2. Samarth Agrawal also took his employer's HFT source code to a competitor. But unlike Aleynikov, Agrawal printed out the code and took the printouts home in a backpack. (These are similar to the facts in *Bottone*, which is discussed in both *Aleynikov* opinions). The Second Circuit upheld his conviction under the NSPA, writing, "Agrawal stole computer code in the tangible form of thousands of sheets of paper ... . This makes all the difference." *United States v. Agrawal*, 726 F.3d 235 (2nd Cir. 2014). Is this right? Should it really matter whether the defendant hits "print" before (Agrawal) or after (Aleynikov) he gets home? What result under New York law?

C. Conversion

THYROFF V. NATIONWIDE MUTUAL INSURANCE CO.

8 N.Y.3d 283 (2007)

Graffeo, Judge:

The United States Court of Appeals for the Second Circuit has certified a question to us that asks whether the common-law cause of action of conversion applies to certain electronic computer records and data. Based on the facts of this case, we hold that plaintiff may maintain a conversion claim.

I

Plaintiff Louis Thyroff was an insurance agent for defendant Nationwide Mutual Insurance Company. In 1988, the parties had entered into an Agent's Agreement that specified the terms of their business relationship. As part of the arrangement, Nationwide agreed to lease Thyroff computer hardware and software, referred to as the agency office-automation (AOA) system, to facilitate the collection and transfer of customer information to Nationwide. In addition to the entry of business data, Thyroff also used the AOA system for personal e-mails, correspondence and other data storage that pertained to his customers. On a daily basis, Nationwide would automatically upload all of the information from Thyroff's AOA system, including Thryoff's personal data, to its centralized computers.

The Agent's Agreement was terminable at will and, in September 2000, Thyroff received a letter from Nationwide informing him that his contract as an exclusive agent had been cancelled. The next day, Nationwide repossessed its AOA system and denied Thyroff further access to the computers and all electronic records

and data. Consequently, Thyroff was unable to retrieve his customer information and other personal information that was stored on the computers.

[Thyroff sued in federal court for conversion. The district court dismissed his claim. On appeal, the court certified a question of state law to the New York Court of Appeals: "is a claim for the conversion of electronic data cognizable under New York law?"]

III ...

Conversion and its common-law antecedents were directed against interferences with or misappropriation of "goods" that were tangible, personal property. This was consistent with the original notions associated with the appeals of robbery and larceny, trespass and trover because tangible property could be lost or stolen. By contrast, real property and all manner of intangible rights could not be lost or found in the eyes of the law and were not therefore subject to an action for trover or conversion.

Under this traditional construct, conversion was viewed as the unauthorized assumption and exercise of the right of ownership over goods belonging to another to the exclusion of the owner's rights. Thus, the general rule was that "an action for conversion will not normally lie, when it involves intangible property" because there is no physical item that can be misappropriated. *Sporn v MCA Records,* 58 N.Y.2d 482, 489 (1983).

Despite this long-standing reluctance to expand conversion beyond the realm of tangible property, some courts determined that there was "no good reason for keeping up a distinction that arose wholly from that original peculiarity of the action" of trover (that an item had to be capable of being lost and found) and substituted a theory of conversion that covered "things represented by valuable papers, such as certificates of stock, promissory notes, and other papers of value" *Ayres v French,* 41 Conn. 142, 150, 151 (1874). This, in turn, led to the recognition that an intangible property right can be united with a tangible object for conversion purposes. *See Agar v Orda,* 264 N.Y. 248, 251 (1934).

In *Agar,* which involved the conversion of intangible shares of stock, this Court applied the so-called "merger" doctrine because: "for practical purposes [the shares] are merged in stock certificates which are instrumentalities of trade and commerce.... Such certificates are treated by business men as property for all practical purposes.' ... Indeed, this court has held that the shares of stock are so completely merged in the certificate that conversion of the certificate may be treated as a conversion of the shares of stock represented by the certificate" 264 N.Y. at 251.

More recently, we concluded that a plaintiff could maintain a cause of action for conversion where the defendant infringed on the plaintiff's intangible property right to a musical performance by misappropriating a master recording—a tangible item of property capable of being physically taken. *See Sporn v MCA Records,* 58 N.Y.2d 482, 489 (1983).[7]

IV

We have not previously had occasion to consider whether the common law should permit conversion for intangible property interests that do not strictly satisfy the merger test. Although some courts have adhered to the traditional rules of conversion, *see e.g., Allied Inv. Corp. v Jasen,* 354 Md. 547, 562, (1999) (interests in partnership and corporation); *Northeast Coating Tech., Inc. v Vacuum Metallurgical Co., Ltd.,* 684 A.2d 1322, 1324 (Me. 1996) (interest in information contained in

prospectus); *Montecalvo v Mandarelli,* 682 A.2d 918, 929 (R.I. 1996) (partnership interest), others have taken a more flexible view of conversion and held that the cause of action can embrace intangible property, *see e.g. Kremen v Cohen,* 337 F.3d 1024, 1033-1034 (9th Cir 2003) (Internet domain name; applying California law); *Shmueli v Corcoran Group,* 9 Misc. 3d 589, 594 (Sup Ct, NY County 2005) (computerized client/investor list); *see generally Town & Country Props., Inc. v Riggins,* 249 Va. 387, 396-397 (1995) (person's name).[8]

A variety of arguments have been made in support of expanding the scope of conversion. Some courts have decided that a theft of intangible property is a violation of the criminal law and should be civilly remediable, *see National Sur. Corp. v Applied Sys., Inc.,* 418 So. 2d 847, 850 (Ala. 1982); that virtual documents can be made tangible "by the mere expedient of a printing key function," *Shmueli v Corcoran Group,* 9 Misc. 3d at 592; that a writing is a document whether it is read on the computer or printed on paper, *see Kremen v Cohen,* 325 F.3d 1035, 1048 (9th Cir 2003) (Kozinski, J., dissenting from certification)); and that the expense of creating intangible, computerized information should be counterbalanced by the protection of an effective civil action, *see National Sur. Corp.,* 418 So. 2d at 850.

On the other hand, the primary argument for retaining the traditional boundaries of the tort is that it "seem[s] preferable to fashion other remedies, such as unfair competition, to protect people from having intangible values used and appropriated in unfair ways." PROSSER AND KEETON, TORTS § 15, at 92. Nonetheless, advocates of this view readily concede that "[t]here is perhaps no very valid and essential reason why there might not be conversion of" intangible property, *id.* at 92, and that there is "very little practical importance whether the tort is called conversion, or a similar tort with another name" because "[i]n either case the recovery is for the full value of the intangible right so appropriated," RESTATEMENT (SECOND) OF TORTS § 242, cmt. *e*. The lack of a compelling reason to prohibit conversion for redress of a misappropriation of intangible property underscores the need for reevaluating the appropriate application of conversion.

V

It is the strength of the common law to respond, albeit cautiously and intelligently, to the demands of commonsense justice in an evolving society. That time has arrived. The reasons for creating the merger doctrine and departing from the strict common-law limitation of conversion inform our analysis. The expansion of conversion to encompass a different class of property, such as shares of stock, was motivated by society's growing dependence on intangibles. It cannot be seriously disputed that society's reliance on computers and electronic data is substantial, if not essential. Computers and digital information are ubiquitous and pervade all aspects of business, financial and personal communication activities. Indeed, this

---

8. At least one court has approved of the use of conversion by referencing the merger doctrine. *See, e.g., Astroworks, Inc. v Astroexhibit, Inc.,* 257 F. Supp 2d 609, 618 (S.D.N.Y. 2003) (conversion of idea that was represented by an Internet Web site). Conversion claims have also been approved without consideration of the historical limits of the cause of action. *See, e.g., Cole v Control Data Corp.,* 947 F.2d 313, 318 (8th Cir. 1991) (computer software program); *Quincy Cablesystems, Inc. v Sully's Bar, Inc.,* 650 F. Supp. 838, 848 (D. Mass. 1986) (satellite cable signals); *Charter Hosp. of Mobile, Inc. v Weinberg,* 558 So. 2d 909, 912 (Ala 1990) (addiction treatment program); *National Sur. Corp. v Applied Sys., Inc.,* 418 So. 2d 847, 850 (Ala. 1982) (computer program); *Mundy v Decker,* 1999 WL 14479, *4, 1999 Neb. App .LEXIS 3, *10-12 (Ct. App. 1999) (WordPerfect documents).

opinion was drafted in electronic form, stored in a computer's memory and disseminated to the Judges of this Court via e-mail. We cannot conceive of any reason in law or logic why this process of virtual creation should be treated any differently from production by pen on paper or quill on parchment. A document stored on a computer hard drive has the same value as a paper document kept in a file cabinet.

The merger rule reflected the concept that intangible property interests could be converted only by exercising dominion over the paper document that represented that interest. Now, however, it is customary that stock ownership exclusively exists in electronic format. Because shares of stock can be transferred by mere computer entries, a thief can use a computer to access a person's financial accounts and transfer the shares to an account controlled by the thief. Similarly, electronic documents and records stored on a computer can also be converted by simply pressing the delete button *Cf. Kremen v Cohen,* 337 F3d at 1034 ("It would be a curious jurisprudence that turned on the existence of a paper document rather than an electronic one. Torching a company's file room would then be conversion while hacking into its mainframe and deleting its data would not." (emphasis omitted)).

Furthermore, it generally is not the physical nature of a document that determines its worth, it is the information memorialized in the document that has intrinsic value. A manuscript of a novel has the same value whether it is saved in a computer's memory or printed on paper. So too, the information that Thyroff allegedly stored on his leased computers in the form of electronic records of customer contacts and related data has value to him regardless of whether the format in which the information was stored was tangible or intangible. In the absence of a significant difference in the value of the information, the protections of the law should apply equally to both forms— physical and virtual.

In light of these considerations, we believe that the tort of conversion must keep pace with the contemporary realities of widespread computer use. We therefore answer the certified question in the affirmative and hold that the type of data that Nationwide allegedly took possession of—electronic records that were stored on a computer and were indistinguishable from printed documents—is subject to a claim of conversion in New York. Because this is the only type of intangible property at issue in this case, we do not consider whether any of the myriad other forms of virtual information should be protected by the tort.

NOTES

1. Does Thyroff have a *tangible* property right, an *intangible* property right, an *intellectual* property right, or something else?
2. Does *Thyroff* only apply to business data, or should it also cover personal files like family photos and recipe collections?
3. What if Thyroff had stored his files in a cloud service operated by Nationwide, and Nationwide had cut off his access? Or what if Nationwide had repossessed the computer with Thyroff's files, but Thyroff still had a copy of all of the files on another computer in his office? What if he kept only paper backups in file cabinets?
4. James Grimmelmann and Christina Mulligan, *Data Property*, 72 Am. U. L. Rev. 829 (2023), argues that a person possesses data, and thus has property rights in it, when they "have … control over a physical instantiation of the data." Is this the right way to describe the situation in *Thyroff*?