AN A.S. PRATT PUBLICATION
NOVEMBER/DECEMBER 2021
VOL. 7 NO. 9

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 7 **NUMBER 9** **November/December 2021**

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at 908-673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3385
Fax Number ..... (800) 828-8341
Customer Service Web site ..... http://www.lexisnexis.com/custserv/
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (937) 247-0293

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY &CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [7] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [293] (LexisNexis A.S. Pratt)

An A.S. Pratt Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2021–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report*, LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

The Evolving Right to Privacy: From Religious Practice to International Tech Branding Tool

By Jason J. Oliveri*

The right to privacy continues to evolve as we create spaces for its relevancy. Beginning first as a religious practice, the right to privacy eventually spilled over into the secular and took on legal meaning. With the rise of information technology, the right to privacy has become more complicated and the United States is now struggling with how to balance it with innovations in technology. This struggle is due, in part, to the United States competition with China. However, the victor in the race for technological supremacy will not necessarily be the most innovative, but instead, the one perceived as being the most trustworthy. This article discusses the right to privacy.

The right to privacy continues to evolve as we create spaces for its relevancy. It certainly did not exist for our tribal ancestors nor did it make much of an appearance in the Middle Ages when it was common for guests to share a single bed with their hosts entire household – servants and the family cat included.[1] At that time, privacy was generally afforded only to those seeking a connection with the divine through spiritual contemplation and prayer, which was thought to be a solitary undertaking.[2] Eventually, this religious practice took on legal significance in the secular world. Everyone is likely familiar with the old proverb, "a man's home is his castle." It can be traced as far back as 1499, appears in the much-quoted Semyane decision from 1604 drafted by English judge and jurist Sir Edward Coke and was later forged into the Bill of Rights, albeit phrased differently and without explicitly referencing a right to privacy.[3]

Approximately 100 years after the U.S. Constitution was adopted, a Boston lawyer by the name of Louis Brandeis, who would later become a Supreme Court Justice, and his partner, Samuel Warren, published an article, "The Right to Privacy," in the Harvard Law Review, which argued that:

> Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual . . .

* Jason J. Oliveri is a partner in Hinshaw & Culbertson's New York office. He advises businesses on compliance with privacy-related laws, rules and regulations and defends financial services companies in state and federal courts against claims arising under the Truth in Lending Act, Home Owners Equity Protection Act, Real Estate Settlement Procedures Act, Fair Debt Collection Practices Act and the Telephone Consumer Protection Act. He can be reached at joliveri@hinshawlaw.

[1] https://medium.com/the-ferenstein-wire/the-birth-and-death-of-privacy-3-000-years-of-history-in-50-images-614c26059e.

[2] *Id.*

[3] *Semayne's Case*, 77 Eng. Rep. 194 (K.B. 1604).

> the right 'to be let alone'. . . . Numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'[4]

While the article was undoubtedly influential – and continues to be to this day – it was not until 1965 that the right to privacy formed the basis of a Supreme Court ruling in the United States.

THE RIGHT TO PRIVACY

In *Griswold v. Connecticut*, a case involving Connecticut's prohibition on the use of contraceptives, Justice William Douglas, writing for the majority, found that there is a right to privacy within the "penumbra of rights" provided through the Constitution, even though it is not specifically identified in one of the amendments.[5] Thereafter, the discussion on privacy in the United States would focus primarily on the right to privacy as it relates to governmental intrusions, particularly in the context of criminal investigations.

This seemingly straightforward notion of a right to privacy became more complicated with the rise of information technology and its ability to collect, store, transfer, and disseminate vast amounts of personal information. Today, the words of Brandeis and Warren have a prophetic ring as we struggle to balance the right to privacy with innovations in technology.

Naturally, we all want the benefits and conveniences that technology can offer, but like most things, technology is a double-edged sword. For example, technology has made applying for credit easier and faster. With just a few clicks on any handheld device you can be approved for a mortgage in minutes. However, without proper safeguards, those same applications and the algorithms that power them can yield discriminatory results based on race, gender, sexual orientation and even an applicant's zip code. As such, managing the negative aspects of technology requires managing personal data and its uses.

THE GDPR

The European Union attempted to tackle this issue with the passage of the General Data Protection Regulation ("GDPR"). Is it perfect? No. Not much, if anything, is. Nevertheless, it was a major step forward in enhancing data privacy rights and protections and is now considered the world's gold standard. By most accounts, Americans want the same protections and just as much control over their personal data as their European counterparts.

---

[4] https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf.

[5] *Griswold v. Connecticut*, 381 U.S. 479, 85 S. Ct. 1678, 14 L. Ed. 2d 510 (1965).

Significantly, a Pew study from 2020 found that 52 percent of Americans decided not to use a product or service because of concerns over data protection.[6] States like California, Colorado, and Virginia have heeded the call and enacted data privacy laws that resemble the GDPR to one degree or another. It is projected that more states will follow suit, creating a patchwork of data privacy laws throughout the country, making it difficult and costly for businesses to comply.

THE FEDERAL TRADE COMMISSION

On top of that, the Federal Trade Commission ("FTC") under the leadership of Lina Kahn, a vocal critic of big tech, has been increasingly active in the space, which will only accelerate. On September 13th the White House announced President Biden's nomination of Alvaro Bedoya, founding director of the Center on Privacy & Technology at Georgetown Law, to serve as a commissioner of the FTC.[7]

The very next day, the FTC announced the passage of eight "omnibus" resolutions to authorize quicker investigations into prioritized issues such as bias in algorithms and biometrics, dark patterns and deceptive online conduct.[8] Shortly thereafter, on September 20th, a group of senators called on Kahn to undertake a rulemaking process to protect consumer data ". . . in parallel to congressional efforts to create federal privacy laws to give power back to consumers. . . ."[9]

In sum, these events suggest that a data privacy and protection law at the federal level could be long in the coming, if at all.

A FEDERAL DATA PRIVACY LAW?

Fearing enforcement from all sides, many businesses are now eager for the guidance and certainty that a federal data privacy and protection law would provide. So, what is stopping the United States from enacting such a law? At least in part, China. In 2015, China announced its "Made in China 2025" plan with the intention of transforming itself from a low-cost manufacturer to a global leader in advanced technologies. Many believe that China has already achieved that goal and that a federal data privacy and protection law would cool innovation and destroy any chance the United States has to compete on the international stage.

---

[6] https://www.pewresearch.org/fact-tank/2020/04/14/half-of-americans-have-decided-not-to-use-a-product-or-service-because-of-privacy-concerns/.

[7] https://www.whitehouse.gov/briefing-room/statements-releases/2021/09/13/president-biden-announces-10-key-nominations-2/.

[8] https://www.ftc.gov/system/files/documents/public_statements/1596260/p859900omnibuslmkrksconcur.pdf.

[9] https://www.blumenthal.senate.gov/imo/media/doc/2021.09.20%20-%20FTC%20-%20Privacy%20Rulemaking.pdf.

In an attempt to counter China's ambitions, the Senate passed the United States Innovation and Competition Act ("ICA"), which if passed by the House and signed into law would pour millions of dollars into technological research and development.[10] However, the ICA will likely not be enough to save any competitive edge that the United States still enjoys. Indeed, the bill's $250 billion price tag is a drop in the bucket compared to what China has reportedly already spent towards achieving its goal.

Given the circumstances, the United States could benefit from thinking about competition in a different way. Indeed, the winner of the technology race is not necessarily going to be the most innovative, but more likely, the one perceived as the most trustworthy. Consider, for example, Lithuania's Defense Ministry's recent recommendation to consumers that they not buy, or throw away as soon as possible, any phones made by China's Xiaomi Corp. because they have built in censorship capabilities.[11] Although the feature was turned off in phones sold in the European Union, the capability remained in place and the resulting concerns were enough to make these Chinese products so untrustworthy they were deemed to be essentially e-waste.

BRANDING PRIVACY

Reading the writing on the wall, many businesses, including giants like Apple and Google, are making privacy part of their brand.[12] It is not uncommon now to go onto a company's website and see a message that says, "we care about your privacy," with a link to an easy-to-read privacy policy nearby outlining how data is used and how consumers can control the use of their data.

Many of these same forward-thinking organizations are also designing products with privacy in mind and are advertising them accordingly.[13] Not only does this help establish trust with consumers, but it acts as a stand-alone, value-add and a way for businesses to distinguish themselves from competitors. Considering the "big tobacco" moment Facebook is currently experiencing, to say nothing of the Snowden leaks, passing a data privacy and protection law at the federal level is just the type of global messaging the United States needs right now to stay competitive. Consumers want it, businesses want it, and it just makes sense.

---

[10] https://www.congress.gov/bill/117th-congress/senate-bill/1260.

[11] https://www.independent.co.uk/news/long_reads/world/lithuania-defence-chinese-phones-censorship-b1924729.html.

[12] *See* https://www.cnbc.com/2021/06/07/apple-is-turning-privacy-into-a-business-advantage.html; *see also* https://www.forbes.com/sites/forbestechcouncil/2021/10/07/why-data-privacy-is-good-for-business-online-privacy-as-a-branding-imperative/?sh=14917d3297ec.

[13] *Id.*