Notre Dame Journal on Emerging Technologies

Volume 3
Issue 1 *Artificial Intelligence*

Article 5

2-2022

Note: Self-Regulation by the Private Industry and its Effectiveness in Today's Online Environment

Stephanie Wong
Notre Dame Law School

Note: Self-Regulation by the Private Industry and its Effectiveness in Today's Online Environment

Erratum

The editors recognize that the page numbers for this Note need to be corrected. The preceding Note by Crane should end on page 166; this Note should be paginated as 167 through 200.

VOLUME 3 FEBRUARY 2022 ISSUE 1

JOURNAL ON EMERGING TECHNOLOGIES

NOTE

SELF-REGULATION BY THE PRIVATE INDUSTRY AND ITS EFFECTIVENESS IN TODAY'S ONLINE ENVIRONMENT

Stephanie Wong

SELF-REGULATION BY THE PRIVATE INDUSTRY AND ITS EFFECTIVENESS IN TODAY'S ONLINE ENVIRONMENT

*Stephanie Wong**

INTRODUCTION

Over 30 years ago, self-regulation served as a hopeful potential regulatory framework that would allow private companies to provide effective privacy protections for consumers. The aspiration for a data protection self-regulation regime arose due to the emergence and development of online commercial activity. E-commerce benefited companies that conducted business online but presented new challenges for the protection of consumer data. The Federal Trade Commission encouraged companies that collect consumer data to develop their own forms of self-regulation to protect the personal data of online consumers. If properly implemented, self-regulation promised efficient reorganization of privacy protections to meet the challenges of online data security from decades ago to now.[1] In response to the Federal Trade Commission's encouragement, several different self-regulatory approaches have emerged with a mix of diverse sector involvement, ranging from governmental to trade associations. Self-regulation is likely to be a fundamental part of consumer data privacy regulation for the foreseeable future. Currently, most online companies rely on a self-regulatory model to police bad behavior that violates general privacy protections for their users. However, the rapid expansion of the Internet and the evolution of the online marketplace calls into question the effectiveness of businesses' present self-regulatory regime and whether these businesses are providing proper privacy protections for online consumers.

As part of the examination of whether existing practices of self-regulation are effective, it is necessary to understand what "self-regulation" is. There are several definitions for the term but in its most basic form, self-regulation means that the "industry or profession rather

*Juris Doctor Candidate, Notre Dame Law School, 2022; Bachelor of Arts in Political Science, Double Minors in English and Asian American Studies, University of Florida, 2016. I would like to thank Professor Patricia L. Bellia for her guidance during the writing process. Thank you to my colleagues on the Notre Dame *Journal on Emerging Technologies* for their diligent effort in editing this piece and all other publications. Finally, I would like to thank my family, partner, and friends for their boundless love, sacrifices, and support. All errors are my own.

[1] Douglas C. Michael, *Federal Agency Use of Audited Self-Regulation as a Regulatory Technique*, 47 ADMIN. L. REV. 171, 188 (1995).

than the government is doing the regulation."[2] Self-regulation is described as a spectrum. On one end, it is a formally delegated power by the government to regulate. On the other end, it is the private sector's responsibility to regulate itself in response to consumer demand or to improve industry reputation.[3] Often, an industry will engage in self-regulation to prevent federal or state government interference. Self-regulation is also undertaken to implement or supplement governmental legislation.[4]

For the purposes of this paper, the "private industry" refers to economic activity in the private sector. The private sector refers to businesses that are owned by citizens rather than owned by the government. This paper focuses specifically on businesses that engage in e-commerce and online activity where general consumer data is collected. General consumer privacy online includes a wide range of privacy issues, including spam, social networking, behavioral advertising, pretexting, spyware, peer-to-peer file sharing, and mobile devices.[5]

This paper will examine present self-regulatory practices that are used by the private industry, and their adequacy in today's Internet landscape. In observing self-regulatory practices, this paper will outline self-regulation, describe the development of the private industry's self-regulation of online consumer privacy up to the present, and provide a recommendation to best achieve general privacy protections for online consumers.

I. UNDERSTANDING SELF-REGULATION

A. Arguments for Self-Regulation

Experts (lawyers, economists, political scientists) argue that there are benefits to self-regulation. This section will further define self-regulation by weighing its advantages. Several advantages include the following: (1) technical expertise and superior knowledge in an industry's subject-area; (2) flexibility in rule development; (3) increased willingness

---

[2] Angela J. Campbell, *Self-Regulation and the Media*, 51 FED. COMM. L.J. 711, 715 (1999).

[3] Larry Irving, *Introduction from the Assistant Secretary, Privacy Report*, NAT'L TELECOMM. & INFO. ADMIN. (1997), https://www.ntia.doc.gov/page/privacy-report-introduction (last visited Jan. 25, 2022).

[4] Campbell, *supra* note 2.

[5] *See generally* FED. TRADE COMM'N, FTC'S USE OF ITS AUTHORITIES TO PROTECT CONSUMER PRIVACY AND SECURITY (2020), https://www.ftc.gov/system/files/documents/reports/reports-response-senate-appropriations-committee-report-116-111-ftcs-use-its-authorities-resources/p065404reportprivacydatasecurity.pdf.

for compliance; (4) potential cost-saving measures for government; and (5) avoidance of unclear legal areas.

Expertise and Superior Knowledge. Self-regulators usually possess superior knowledge of their industry and its related subjects compared to a government agency. Private companies are comprised of "individuals or groups with an interest in and knowledge of the subject area around which they are organized."[6] It is arguably more efficient for the government to rely on this already existing, collected expertise rather than reproduce it within a governmental agency. Reproduction would likely be time-consuming and costly.

Flexibility. Self-regulators retain flexibility since they can modify and update their rules. There are various reasons why rules may need to be updated, for example, an industry may have technological changes and advancements. Companies can quickly change their rules to promote their products or goals. This is because private companies typically possess less rigid and informal structures compared to the formality of the government. Private companies are better able to respond to changes while government agencies are often required to navigate rigid bureaucratic agencies and rulemaking policies. Government agencies are bound to notice and comment procedures,[7] which can be time-consuming and arduous.

Willingness to Comply. Since self-regulators develop rules from their own expert knowledge base in their respective industry, members of their industry perceive these rules as more reasonable in comparison to government-issued rules. Self-regulators will likely feel more inclined to comply with these rules because their own peers developed them. These industry-developed rules will likely be consistent with the entity's goals and not impair or inhibit company production, increasing willingness for compliance.[8]

Cost-saving for the Government. Self-regulation can be cost saving for the government. Self-regulation only occurs if its cost requires fewer resources from the government than direct regulation. Since governments often do not possess the requisite and technical expertise that the private industry has, they must spend resources on attaining or training staff on the necessary knowledge. This takes time and money. Instead, these costs can be placed on the private industry. Although it is likely that the government may still be involved in some capacity—e.g., through supervision of the overall regulatory process—that often requires less resources than direct regulation. However, self-regulation is cost saving for the government only if the net reduction in cost to the private industry is lower than the government's cost savings.[9]

Prevents Legal Challenges. Self-regulation can be beneficial when rules or adjudicatory procedures are challenging or confusing to apply in

---

[6] Michael, *supra* note 1, at 181.
[7] 5 U.S.C. § 553.
[8] Campbell, *supra* note 2, at 716.
[9] *Id.*

certain scenarios. This argument is made with respect to the ever-evolving practice area of cyberlaw, where jurisdictional and sovereignty issues make it difficult for governments to enforce its laws.[10] Instead of tracking down points of contact for an online transaction that may have interacted with several computers, networks, and cloud storage to determine proper jurisdiction, private companies can enforce their industries' rules and avoid these confusing legal rules.

B. Arguments Against Self-Regulation

Self-regulation is not without its shortcomings, which will be discussed in this section. The same experts discussed in the previous section have also identified arguments against self-regulation by the private industry. The arguments against self-regulation are as follows: (1) self-regulation can potentially result in inadequate enforcement since private companies are left in charge of their own regulatory implementation; (2) even with proper implementation, self-regulation increases the amount of unreviewable discretion exercised by the self-regulator; (3) Congress likely has limitations on the type of regulations that it can delegate to the private industry; (4) the private industry's priorities will likely take higher precedence than its consumers' interests; (5) and lastly, self-regulation amongst powerful private companies will likely result in antitrust issues.[11]

Inadequate Enforcement. First, self-regulation raises the possibility of inadequate enforcement of a regulatory program because the regulated entities are left directly or indirectly in charge of implementation. Self-regulation causes an industry to standardize conduct throughout its membership. This is risky because industry members may violate their peer-developed rules for the success of their business. Additionally, these private companies may be unwilling to commit the resources required for effective self-regulation as it may be costly. The enforced penalties for regulatory violations may be inadequate to cause a private company to completely comply. The most severe potential penalty for noncompliance consists of trade association expulsion, which may be an ineffective deterrent if the benefits of membership are insignificant. In many cases, enforcement by trade associations often result in denial of the right to display a seal, which can be insufficient.[12]

Exercise of Unreviewable Discretion. Self-regulation gives companies the flexibility to "tailor enforcement to particular industries or practices."[13] This flexibility produces an increase in discretion by

---

[10] *See generally* David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996).
[11] Michael, *supra* note 1, at 189.
[12] Campbell, *supra* note 2, at 718.
[13] Michael, *supra* note 1, at 190.

companies to over and under regulate as they please. It is difficult to measure what an "ideal" amount of discretion looks like. It is also difficult to measure the benefits of discretion and the potential harm of unreviewable discretion.[14] Limitations on the amount of discretion exercised would help in these situations but enforcement may be inadequate.

Political Restrictions on Delegation. There may be certain subject areas that industries are unable to self-regulate because of existing regulatory frameworks by congressional oversight of agencies.[15] It is unlikely that Congress would remove these subject areas from its purview thus potentially limiting the extent of self-regulation.[16]

Industry Priorities. While industry may possess greater technical expertise than government, companies may employ their expertise to maximize the industry's profits.[17] These companies may "confuse self-regulation with self-service."[18] Self-regulators may fail to pay attention to other affected parties outside their industry. Regulations should advance the public interest and the interests of regulated entities. A business's desire for profits may outweigh the needs of the public.

Antitrust Issues. Lastly, self-regulation can facilitate anticompetitive conduct. Self-regulation typically involves competitors in an industry getting together to agree on how they will conduct their business. This type of agreement raises antitrust issues when important elements of competition are restricted. Agreements by professional organizations have sometimes been challenged by the government under antitrust law.[19] Liability has been found when companies have abused their self-regulatory processes. Examples include packing numerous representatives from a single company on a standard-setting self-regulatory committee. Similarly, the lack of an appropriate process for

---

[14] *Id.*

[15] *Id.* at 250 n.93 ("William Cary, generalizing from his experience as Chairman of the Securities and Exchange Commission, concluded that "[i]t may seem lacking in courage, but I believe it is safe to conclude that agencies seldom take controversial steps under their rule making power which do not have some support from Congress.").

[16] *See id.* at 250 n.94 ("[An] example is the Department of Agriculture's meat inspection system. Although physical inspection of each animal slaughtered is required by law, *see* 21 U.S.C. §§ 604-605 (1988), such inspection is not effective in identifying bacterial infestations that are today considered a primary cause of food-borne illnesses [...] Congress rebuffed the Department's attempts to modify the physical inspection system, ultimately removing all funding for the program.").

[17] Campbell, *supra* note 2, at 717.

[18] *See* DONALD I. BAKER & W. TODD MILLER, NAT'L TELECOMM. & INFO. ADMIN., PRIVACY, ANTITRUST AND THE NATIONAL INFORMATION INFRASTRUCTURE (1997), https://www.ntia.doc.gov/page/chapter-2-antitrust-considerations#N_1_.

[19] *See* JOSEPH KATTAN & CARL SHAPIRO, U.S. DEP'T OF COM., PRIVACY, SELF-REGULATION, AND ANTITRUST, IN PRIVACY AND SELF-REGULATION IN THE INFORMATION AGE (1997).

reviewing self-regulatory abuses by companies has been found to be anticompetitive.[20]

II. SELF-REGULATION OVER TIME AND THE CURRENT APPROACH

This section of the paper will examine the development of the private industry's self-regulation from the advancement of the Internet in the 1990s up to its current state of play. Specifically, this section will examine the evolution of general consumer privacy self-regulation. Currently, the landscape of self-regulation is a "mix of sector-specific statutes, administrative action, and self-regulation."[21] This landscape resulted for various reasons. First, certain states have reacted to the lack of comprehensive privacy legislation and have enacted their own state laws. Sector-specific statutes have also developed in reaction to online privacy concerns that have developed with the expanse of the Internet. Second, the Federal Trade Commission (FTC) has statutory authority to protect consumers from unfair and deceptive commercial practices. The Commission has acted to protect consumers' online privacy by developing fair information practices and investigating companies. Furthermore, the FTC's investigations and statutory authority has produced a body of "common law" that is influential to private companies who look to the FTC for guidance for privacy protection standards. Third, the FTC has called for self-regulation by the private industry. In the shadow of the FTC's guidance, various self-regulatory regimes developed.

A. Existing Sector-Specific Statutes

There are currently several areas of online activity that are already federally regulated. Therefore, private companies are prevented from self-regulating in the subject areas mentioned hereafter and must comply with these federal mandates.

Children's Online Privacy Protection Act (COPPA) regulates the use and collection of data for children under the age of thirteen.[22] COPPA is aimed towards website operators who knowingly collect minors'

---

[20] *See generally* David A. Balto, *Protecting Privacy Through Self-Regulation: Avoiding Antitrust Risks, Electronic Banking Law and Commerce Report*, 6 NO. 5 ELEC. BANKING L. & COM. REP. 7, 7-13 (Oct. 2001).

[21] PATRICIA L. BELLIA, PAUL SCHIFF BERMAN, BRETT M. FRISCHMANN & DAVID G. POST, CYBERLAW: PROBLEMS OF POLICY AND JURISPRUDENCE IN THE INFORMATION AGE 528 (5th ed. 2018).

[22] Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–6502.

information. COPPA urges for parental consent mechanisms for children's digital behaviors.[23]

Other examples of federally regulated online activity include: The Health Portability and Accountability Act (HIPAA) privacy rule protects individual medical records and "requires appropriate safeguards to protect the privacy of personal health information."[24] The Family Education Rights and Privacy Rights Act of 1974 (FEPRA) restricts access to students' educational records.[25] The statute allows students to control who has access to their data. FEPRA does not provide protections beyond students' educational records.[26] The Fair Credit Reporting Act (FCRA) protects the privacy of consumer report information and requires that consumer reporting agencies supply accurate information. The FCRA holds accountable those that handle this type of information with legal obligations and potential consequences.[27] The Gramm-Leach-Bliley Act requires financial institutions to explain their information-sharing practices to their consumers and to safeguard sensitive data.[28]

Several states have implemented or introduced their own privacy legislation including California, New York, Maryland, Virginia, Washington, and Hawaii. States continue to propose data privacy legislation and various federal bills have been proposed over the last few years.[29]

B. Administrative Regulation by the Federal Trade Commission

It is difficult to discuss the evolution of private companies' self-regulation without mentioning the impact that the FTC had on self-regulatory development. The 1990s saw an expansion of the Internet and e-commerce.[30] Online commercial activity boomed, and websites could easily collect personal consumer data. Collection of personal consumer data gave rise to data privacy concerns. This development transformed

---

[23] Regulation of unfair and deceptive acts and practices in connection with collection and use of personal information from and about children on the Internet. 15 U.S.C. § 6502.

[24] *The HIPAA Privacy Rule*, HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/privacy/index.html (last visited on Jan. 23, 2022);
Health Insurance Portability and Accountability Act, 42 U.S.C § 1320(d).

[25] Family Education and Rights Privacy Act of 1974, 20 U.S.C. § 1232g.

[26] *Id.*

[27] Fair Credit Reporting Act, 15 U.S.C. §§ 1681-1681x.

[28] Gramm-Leach-Bliley Act of 1999, 113 Stat. 1338.

[29] *See* Consumer Data Protection Act, S. 2188, 115th Cong. (2018); Data Care Act of 2018, S. 3744, 115th Cong. (2018); American Data Dissemination Act of 2019, S. 142, 116th Cong. (2019).

[30] Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 2235, 2235 (2015) [hereinafter *FTC Data Protection*].

the marketplace, and many consumers began to become wary of using the Internet.[31] With a lack of involvement by Congress and a dearth of laws, companies developed their own self-regulatory regimes under the guidance of the FTC.[32]

Under Section 5(a) of the FTC Act, "unfair or deceptive acts or practices in or affecting commerce…are…declared unlawful."[33] Using its enforcement powers under Section 5, the FTC has pursued privacy violations that are "deceptive" and "unfair" trade practices.[34] The Commission has sought to understand the changing Internet marketplace to safeguard consumers. Inevitably, the FTC filled a hole for consumer protection that a lack of laws generated.

1. Fair Information Practices

In June 1998, the FTC submitted a report to Congress called *Privacy Online: A Report to Congress*.[35] In this report, the FTC explained its efforts to better understand the online marketplace. The Commission conducted workshops and hearings with interested parties to get a better understanding of how industries are protecting consumers' privacy online. The FTC also stated its goal was to encourage and facilitate effective self-regulation in this subject area. In this report, the Commission summarized widely accepted principles of fair information practices for online consumer privacy. The principles were "essential to ensuring that the collection, use, and dissemination of personal information [is] conducted fairly and [is] consistent with consumer privacy interests."[36] The core principles that the FTC assessed are as follows:

> i. **Notice/Awareness:** Consumers should be given notice of a company's information practices before personal information is collected from them to allow consumers to make an informed decision to the extent of disclosure of personal information.[37]

---

[31] *See also* FED. TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS 3 (June 1998) https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf [hereinafter PRIVACY ONLINE].
[32] *FTC Data Protection*, *supra* note 30.
[33] Federal Trade Commission Act, 15 U.S.C. § 45(a)(1).
[34] Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 599 (2014) [hereinafter *New Common Law of Privacy*].
[35] PRIVACY ONLINE, *supra* note 31.
[36] *Id.* at ii.
[37] *Id.* at 7.

ii. **Choice/Consent:** This principle encourages that options are provided to consumers as to how any personal information may be collected from them. This typically takes the form of an opt-in or opt-out or yes/no options that allows consumers to take an affirmative step to exercise their choice.[38]

iii. **Access/Participation:** A consumer should have the ability to access data about themselves and to contest its accuracy and completeness. Access should be timely and inexpensive to consumers.[39]

iv. **Integrity/Security:** Data collectors must take reasonable steps to ensure that data be accurate and secure. This principle calls for the protection against unauthorized access, destruction, use, or disclosure of consumer data. Companies should take effective measures to ensure security of consumer data.[40]

v. **Enforcement/Redress:** To ensure that the fair information practice principles outlines are not just suggestive but effective, enforcement is necessary to prevent violations or unlawful use of consumer data.[41]

a. **Self-Regulation:** For self-regulation to be effective, it must possess both enforcement and redress for injured parties. Here, the FTC recommended several actions that industries could take to ensure successful self-regulatory regimes. Industry associations that conditions memberships on acceptance and compliance of a code of fair information practices; audits conducted by third-party entities to ensure compliance with the principles; and certification of companies that have successfully adopted and complied with the code of fair information practices.[42]

Redress should provide institutional mechanisms to address consumers' concerns. Consumers should have a method to submit complaints and an investigation should follow. Remedies for violations should compensate consumers for any harm suffered and typically take the form of monetary sanctions.[43]

---

[38] *Id.* at 8.
[39] *Id.* at 9.
[40] *Id.* at 10.
[41] *Id.*
[42] *Id.*
[43] *Id.* at 11.

b. **Private Remedies:** The FTC suggested that a statutory scheme could create a private right of action for consumers who are harmed by unfair privacy practices. This could incentivize companies to adopt fair information practices since monetary compensations could be at risk.[44]

c. **Government Enforcement:** Government enforcement through civil or criminal penalties is another option to ensure fair privacy practices by companies.[45]

After the FTC's development of these principles, it surveyed companies to assess industry efforts in adopting these basic fair information practice principles. The Commission concluded that effective industry self-regulation had not taken hold yet. The report concluded with the FTC encouraging the adoption of legislation to protect the online collection of children's information. The report further emphasized the need for industries to implement fair information practices and to adopt self-regulatory regimes to develop a thriving and safe online marketplace that consumers would feel secure engaging in.[46]

In 1998, FTC officials stated before Congress that the FTC was hopeful that self-regulation would "achieve adequate online privacy protections for consumers."[47] At this time, the Commission suggested that Congress refrain from passing legislation regarding consumer privacy.

In May of 2000, the FTC issued another report to Congress entitled *Privacy Online: Fair Information Practices in the Electronic Marketplace*.[48] This report reoutlined the FTC's Fair Information Practice (FIP) principles from its 1998 report and noted that industries were slowly adopting these guidelines.[49] The report called for further industry efforts to implement these principles and promised that the FTC would continue to monitor the progress.[50] Remarkably, in this report the FTC recommended that Congress enact legislation to ensure adequate

---

[44] *Id.*
[45] *Id.*
[46] *Id.* at 43.
[47] FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE, 34 (May 2000), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf [hereinafter FAIR INFORMATION PRACTICES].
[48] *Id.*
[49] *Id.* at 5.
[50] *See generally id.*

protection of *all* consumers' privacy online.[51] The Commission suggested that industry self-regulation should play an important role in any legislative framework.[52]

On December 20, 2007, the FTC released proposed principles for self-regulation[53] that were intended to address consumer privacy concerns related to behavioral advertising, while balancing support for innovation in the online environment.[54] These 2007 principles were an iteration of the 1998 FIPs for consumer privacy.[55] The Commission recognized that many websites collect consumers' data by tracking their online activity. Through this monitoring websites deliver targeted advertising to consumers. In the same press release, the FTC encouraged companies to have meaningful and enforceable self-regulation to address the privacy concerns that can arise from the collection of consumer data for targeted advertising.[56]

The goals of the Principles were to encourage industries to develop meaningful self-regulation in this area of privacy. These Principles are guidelines for self-regulation and do not oblige companies to comply with certain laws. The following are the proposed FTC principles:

> i. **Transparency and consumer control:** This principle calls for a "clear, consumer-friendly, and prominent statement" that consumer data is being collected for the purposes of providing targeted advertising.[57] Consumers should be given the ability to choose whether they want to have their information collected for that purpose.
>
> ii. **Reasonable security, and limited data retention, for consumer data:** Companies should provide reasonable security for any consumer data they collect. They should also only retain the data for as long as is necessary for the business purpose.

---

[51] *Id.* at i.
[52] *Id.* at 36.
[53] FED. TRADE COMM'N, ONLINE BEHAVIORAL ADVERTISING: MOVING THE DISCUSSION FORWARD TO POSSIBLE SELF-REGULATORY PRINCIPLES (Dec. 20, 2007), http://www.ftc.gov/os/2007/12/P859900stmt.pdf.
[54] Press Release, Fed. Trade Comm'n, FTC Staff Proposes Online Behavioral Advertising Privacy Principles (Dec. 20, 2007), http://www.ftc.gov/opa/2007/12/principles.shtm.
[55] PRIVACY ONLINE, *supra* note 31, at 7-11; *supra* notes 37-45. There is a similarity between the proposed privacy principles in the 2007 press release and the principles iterated in the FTC's 1998 *Privacy Online Report*. Both focus on the importance of choice, consent, and self-regulation.
[56] *Supra* note 54.
[57] THEODORE L. BANKS & FREDERICK Z. BANKS, *FTC Proposed Online Behavioral Advertising Policy Principles*, *in* CORPORATE LEGAL COMPLIANCE HANDBOOK § 9.17 (3d ed. 2021–2, Supp. 2020).

> iii. **Affirmative express consent for material changes to existing privacy promises:** Companies must ensure that they obtain affirmative express consent from consumers when they plan to use previously collected data in a manner materially different from promises made when data was initially collected.
>
> iv. **Affirmative express consent to (or prohibition against) using sensitive data for behavioral advertising:** Companies should obtain affirmative consent from consumers before collecting sensitive data to conduct targeted advertising.[58]

These Principles served as guidelines to self-regulatory organizations for online businesses. The Principles have also been revised since 2007, with alterations to the third principle.[59] This change requires affirmative consent from consumers before their data is used in a manner that is "materially different" from the promises the company made when collecting the data.[60] The online marketplace and advancement of technology that makes e-commerce possible have continued to change over the last thirty years. Given the dynamic nature of the online marketplace, the Commission consistently seeks to avoid stifling innovation so that responsible business practices can continue to develop and flourish. To achieve these objectives, the FTC engages in a continuous dialogue with members of industry, privacy advocates, technology experts, consumers, and interested parties.[61]

2. The FTC's "Common-Law"

Starting in the 1990s, the FTC and its staff have conducted investigations and have brought law enforcement actions challenging deceptive privacy claims and improper disclosure of consumer data.[62] In 2006, the FTC created the Division of Privacy and Identity Protection

---

[58] *Id.*

[59] *Id.* ("The FTC 2009 report on online behavioral advertising which included some revisions to the principles announced in December 2007.").

[60] *Id.*

[61] *See* FED. TRADE COMM'N, SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING, BEHAVIORAL ADVERTISING, 4 (Feb. 2009), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf [hereinafter SELF-REGULATORY PRINCIPLES].

[62] FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE, 3 (Dec. 2010), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf [hereinafter PROTECTING CONSUMER PRIVACY].

(DPIP), which focuses on addressing cutting-edge consumer privacy matters through enforcement, policy development, and outreach to consumers and businesses.[63] The DPIP oversees the following issues: consumer privacy, credit reporting, identity theft, and information security.[64] The DPIP also enforces Section 5 of the FTC Act, the Fair Credit Reporting Act, the Gramm-Leach-Bliley Act, the Children's Online Privacy Protection Act, and the Health Breach Notification Rule.[65]

The Commission has filed complaints against companies who breach their own privacy policies under the FTC Act's unfairness rationale.[66] The FTC also issues reports focusing on online data collection practices, online businesses' self-regulatory efforts, and technological efforts to enhance consumer privacy.[67] As a result of the FTC's privacy enforcement, the FTC is viewed as the *de facto* federal authority for data protection. Countless privacy lawyers and companies consider the FTC as the designated agency that has the power to enforce privacy laws. Therefore, these lawyers and companies scrutinize the FTC's actions to guide their decisions.[68]

Because of the FTC's role in enforcing privacy, scholars argue that the FTC's privacy jurisprudence has developed a privacy "common-law."[69] The Commission has issued over 170 privacy-related complaints against private companies, with every complaint mostly ending up dropped or settled. These complaints and settlements effectively function as a common law, which in American jurisprudence develops precedent and predictability in the development of rules.[70] While the FTC's settlements technically lack precedential force for companies, its decisions have remained consistent and do not stray far away from previous orders. Therefore, private companies have looked to the FTC settlements as they would for precedential judicial decisions.

The FTC's treatment of companies that it brings complaints against has been somewhat predictable. Using the self-regulatory approach to consumer privacy that the FTC recommended companies undertake, the Commission would bring claims against companies that

---

[63] FED. TRADE COMM'N, THE FTC IN 2007: A CHAMPION FOR CONSUMERS AND COMPETITION 28 (Apr. 2007), https://www.ftc.gov/sites/default/files/documents/reports_annual/annual-report-2007/chairmansreport2007_0.pdf.
[64] *Division of Privacy and Identity Protection*, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection/our-divisions/division-privacy-and-identity (last visited Jan. 23, 2022).
[65] *Id.*
[66] *See* 15 U.S.C. § 45(a)(1).
[67] SELF-REGULATORY PRINCIPLES, *supra* note 61, at i.
[68] *New Common Law of Privacy*, *supra* note 34, at 600.
[69] *Id.* at 627.
[70] Frank B. Cross, *Identifying the Virtues of the Common Law*, 15 SUP. CT. ECON. REV. 21, 38 (2007).

failed to live up to the promises that companies voluntarily made in their privacy policies.[71] The FTC's claims alleged that companies were engaging in a deceptive trade practice.[72] Another common tactic the FTC has taken is bringing a complaint against a company that has suffered a data breach, and announcing the fair information practices the company should have followed to avoid the breach.[73] Critics have argued that the FTC should publish rules that give regulated parties fair notice.[74] The FTC has responded that they opt to defer to businesses that collect consumer data for setting the appropriate standards since data security and technology changes too quickly. Ironically, this argument returns to the Fair Information Practice principles that the FTC had begun recommending for companies to follow in 1998. Companies that the FTC has brought claims against have generally settled or dropped their case with the FTC. [75]

The FTC's authority in regulating deceptive and unfair practices is general and expansive.[76] This authority has been established by case decisions. A notable case that has set this precedential authority for the Commission is *FTC v. Wyndham World Corp.*[77] The FTC claimed Wyndham was engaging in deceptive practices by failing to take reasonable steps to protect its consumers' data. Wyndham suffered three breaches which resulted in more than 619,000 consumers' credit card accounts becoming compromised. The FTC alleged that consumers and businesses suffered financial injury due to unreimbursed fraudulent charges, lost access to funds or credit, and increased costs. Wyndham did not settle with the FTC unlike nearly all other defendants have in FTC actions. The FTC brought the action to federal court where Wyndham made three arguments:

> (1) the FTC unfairness authority does not extend to data security; (2) the FTC has failed to give fair notice of what data security practices are required by law; and (3) Section 5 does not apply to the security of payment card data because there is no possibility for consumer injury.[78]

---

[71] *FTC Data Protection*, *supra* note 30, at 2230.
[72] *Id.* at 2235.
[73] *Id.* at 2258.
[74] *Id.*
[75] *New Common Law of Privacy*, *supra* note 34, at 610.
[76] *FTC Data Protection*, *supra* note 30, at 2247.
[77] Fed. Trade Comm'n v. Wyndham Worldwide Corp., 799 F.3d. 236 (3d Cir. 2015).
[78] Fed. Trade Comm'n v. Wyndham Worldwide Corp., 10 F.Supp.3d 602 (D.N.J. 2014).

The U.S. District Court for the District of New Jersey resolved each of these arguments in favor of the FTC. Wyndham appealed the decision and argued the following: that because Congress enacted sector-specific data security laws, Congress did not intend for the FTC to regulate data security under the FTC Act; the FTC must "set data-security standards in advance so that businesses can fairly know what is required of them before the FTC seeks to hold them liable;"[79] and that the FTC's standards were vague and do not indicate what is required of businesses. The Third Circuit only took up the fair notice challenge and found that Wyndham's argument was not persuasive. *FTC v. Wyndham* established FTC's authority under section 5 and set a precedent for other companies to follow.

Facebook's $5 billion penalty set by the FTC was regarded as unpredicted behavior.[80] The FTC charged Facebook with deceiving users about its ability to control the privacy of users' personal information.[81] The settlement imposed unprecedented new restrictions on Facebook's business operations and required Facebook to restructure its approach to privacy from the top-down to improve oversight. The $5 billion penalty is a record-breaking penalty for the FTC with the second-highest penalty at $275 million from a settlement with Equifax.[82] The high penalty was intended to change Facebook's culture and its treatment toward users' privacy. Facebook gets most of its revenue from monetizing user information through targeted advertising. In 2018, Facebook had $55.8 billion in revenues, mostly generated from this targeted advertising.[83]

These cases have established a precedent that likely any case brought by the FTC is a losing battle for the defendant company. The FTC's "common law" recommends that companies follow the appropriate standards set by their industry in protecting consumers' privacy. However, the FTC's principles have set the appropriate standards that guide companies. Arguably, there is no true self-regulation at play for private industries. The FTC has become a dominant enforcer of privacy because its framework was uniquely compatible with the self-regulatory approach that businesses have undertaken. Under self-regulation, private companies developed their own privacy policies which outlined their processes for data collection, use, and disclosure. However, the

---

[79] *FTC Data Protection*, *supra* note 30, at 2240.
[80] Press Release, Fed. Trade Comm'n, FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook (July 24, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions.
[81] *Id.*
[82] *Id.*
[83] *Id.*

private companies' privacy policies often lacked penalties or consequences if they violated their own processes. The FTC has taken the role of oversight and enforcement for companies that fail to follow their self-regulatory models. Described as a "lynchpin" for businesses' self-regulatory approach, the Commission has given legitimacy and credibility to this regime.[84] Thanks to the Commission, the self-regulatory approach for consumer privacy is not an empty promise.[85]

C. Self-Regulation in the Shadow of the FTC

With the guidance and authority of the FTC, the private industry has attempted to self-regulate in the shadow of the Commission. The private sector has taken the FTC's principles and attempted to implement them into their own industry. An approach that the private industry has taken is the development of separate entities that monitor and review companies' privacy policies and practices. The Network Advising Initiative and Global Network Initiative are the results of this approach. These two groups are membership organizations created for their specific industries. They serve as a form of objective governance that requires its members to meet certain standards to be considered trustworthy. Third, is the Third-Party "Trust" Authority, which is a seal-program whose stamp of approval was initially recommended by the FTC. Finally, this section of the paper closes with an examination of a contemporaneous illustration of Facebook's recent attempt to self-regulate in the shadow of its FTC settlement.

1. The Network Advising Initiative

The Network Advising Initiative (NAI) is a non-profit organization and leading self-regulatory association comprised of third-party digital advertising companies.[86] Its mission is to promote a healthy online ecosystem by "maintaining and enforcing high standards for data collection and use for advertising online."[87] Founded in 2000, NAI supports industry self-regulation and states that its members demonstrate a commitment to consumer privacy. Some notable members include Adobe, Google, Microsoft, Oracle, Salesforce, and Verizon Mobile.

In December 2008, the NAI issued a press release announcing that it had adopted an enhanced Self-Regulatory Code of Conduct that is

---

[84] *New Common Law of Privacy*, *supra* note 34, at 604.
[85] *Id.*
[86] *About the NAI*, NAT'L ADVERT. INITIATIVE, https://www.networkadvertising.org/about-nai/ (last visited May 6, 2021).
[87] *Id.*

binding on members which has been updated regularly.[88] The NAI Code mandates that its web-based members provide users a means to opt-out of Internet-Based Advertising.[89] The NAI has a list of data that is deemed sensitive and requires opt-in consent. Opt-in consent is "an affirmative action taken by a user that manifests the intent to opt into an activity described in a clear and conspicuous notice."[90] A user would provide this consent when they are interacting directly with an NAI member.[91] Internet-Based Advertising refers to targeted advertising that results from the collection and use of personal consumer data. This collection of data results in specific advertisements that are tailored based on the interests inferred from the collection of personal consumer data.[92]

NAI members are responsible for setting opt-out cookies for their consumers. The NAI Code requires that the Opt-In Consent be "clear and conspicuous," put users on notice, and instruct users on how to find a more detailed privacy policy for more information. [93] It is recommended the Opt-In message be accompanied with statements of where data sharing may occur and who data may be shared with. This recommendation has resulted in the popular interstitial that pops-up on a company's website.[94]

The NAI conducts an annual review for its members and may recommend sanctions for members who violate this requirement. Examples of the types of sanctions that the NAI can apply are suspension or revocation of membership, public reprimand for the violation, and referral of the matter to the FTC.[95] In 2020, NAI posted its latest membership requirements in its latest Code of Conduct, which are as follows:

> i. **Education**: Members shall maintain an NAI website that offers education about tailored advertising, the requirements of the NAI code, and information about user choices. Members shall make reasonable efforts to educate

---

[88] *See* NAT'L ADVERT. INITIATIVE, 2008 NAI PRINCIPLES CODE OF CONDUCT (Dec. 16, 2008), http://www.networkadvertising.org/networks/2008%20NAI%20Principles_final%20for%20Web site.pdf.

[89] *See* NAT'L ADVERT. INITIATIVE, GUIDANCE FOR NAI MEMBERS: OPT-IN CONSENT (Nov. 2019), https://www.networkadvertising.org/sites/default/files/nai_optinconsent-guidance19.pdf.

[90] *Id.* at 3.

[91] *Id.*

[92] *See id.* at 3.

[93] *Id.* at 2.

[94] *Id.* at 3-6.

[95] NAT'L ADVERT. INITIATIVE, *supra* note 86.

users about tailored advertising and their options available regarding tailored advertising. [96]

ii. **Transparency and Notice:** Members shall provide "clear, meaningful, and prominent notice on its website that describes its data collection, transfer, and use practices" for tailored advertising.[97]

iii. **User Control:** Users should have a level of choice when the member website intends to use sensitive data. This can take the form of an Opt-Out mechanism.[98]

iv. **Use Limitations:** Members shall not create any tailored advertising for users under the age of 16 without parental consent.[99]

v. **Transfer Restrictions:** Members shall contractually ensure that any unaffiliated parties, for which sensitive consumer data is provided, adhere to the NAI Code of Conduct. These parties shall also be contractually prohibited from attempting to re-identify individual users for online advertising purposes without obtaining the user's consent.[100]

vi. **Data Access, Quality, Security, and Retention:** Members shall provide users with reasonable access to their personally identifiable information and shall provide the option for users to opt-out from further targeted advertising. Members shall provide due diligence that the data they obtain are from responsible sources and that reasonable security measures are used to protect data.[101]

These NAI developed principles parallel to the FTC's guidelines for self-regulation. Coming out one year after the FTC's report, it is evident that industries attempted to structure their self-regulatory regimes in the shadow of the FTC's influence.

2. Global Network Initiative

The Global Network Initiative (GNI) is an international organization that was formed in 2008.[102] It is a membership-based organization that focuses on preventing Internet censorship by

---

[96] NETWORK ADVERT. INITIATIVE, 2020 NAI CODE OF CONDUCT 10 (2020), https://www.networkadvertising.org/sites/default/files/nai_code2020.pdf.
[97] *Id.* at 10-12.
[98] *Id.* at 13-14.
[99] *Id.* at 14.
[100] *Id.* at 15.
[101] *Id.* at 15.
[102] *See About GNI,* GLOB. NETWORK INITIATIVE, https://globalnetworkinitiative.org/about-gni/ (last visited Jan. 23, 2022).

governments and protecting the online privacy rights of individuals.[103] GNI is based on internationally recognized human rights laws such as the International Covenant on Civil and Political Rights, which was set out in the Universal Declaration of Human Rights.[104] GNI boasts some notable members such as Google, Meta, Microsoft, Nokia, Verizon Media, and Vodafone.[105]

GNI's main principles are freedom of expression and privacy.[106] Under its privacy principle, privacy is defined as a human right and guarantor of human dignity.[107] Privacy is essential for maintaining personal security, protecting identity, and promoting freedom of expression in the digital age.[108] Everyone should be free from illegal or arbitrary interference with the right to privacy.[109] The right to privacy should not be restricted by governments, except in narrowly defined circumstances based on internationally recognized laws and should be consistent with international human rights laws.[110]

Members of GNI are expected to protect users' personal information from governmental demands or regulations that are illegal.[111] This will be done by "employ[ing] protections with respect to personal information in all countries where [the members] operate to work to protect the privacy rights of users."[112] When confronted with government demands, laws or regulations that compromise privacy in a manner that violates internationally recognized laws and standards, the member must respect and protect the privacy rights of its users.[113] GNI is concerned with protecting users' personal information from

---

[103] *See id.*
[104] International Covenant on Civil and Political Rights, Dec. 19, 1966, 999 U.N.T.S. 172.
[105] *See Our Members, Fellows & Observers*, GLOB. NETWORK INITIATIVE, https://globalnetworkinitiative.org/#home-menu (last visited Jan. 23, 2022).
[106] *See The GNI Principles,* GLOB. NETWORK INITIATIVE, https://globalnetworkinitiative.org/gni-principles/ (last visited Jan. 23, 2022).
[107] *Id.*
[108] *Id.*
[109] *Id.*
[110] *Id.*
[111] The NAI took their definition of illegal or arbitrary interference from the government from Article 12 of the Universal Declaration of Human Rights ("No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.") and Article 17 of the International Covenant on Civil and Political Rights ("(1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation; (2) Everyone has the right to the protection of the law against such interference or attacks."). G.A. Res. 217 (III) A, Universal Declaration of Human Rights, art. 12 (Dec. 10, 1948); International Covenant on Civil and Political Rights, *supra* note 104, art. 17.
[112] The GNI Principles, GLOB. NETWORK INITIATIVE, https://globalnetworkinitiative.org/gni-principles/ (last visited May 6, 2021).
[113] *Id.*

governmental interference. These concerns are valid as companies do not want to get entangled with governmental entities that violate users' human rights principles.[114]

GNI serves as another form of self-regulation for private companies similarly to NAI. The main difference with NAI is that GNI serves as a global trade association, while NAI caters towards U.S. companies. Additionally, NAI pulls inspiration in developing its principles from the FCC's FIPs and GNI pulls inspiration from the United Nations Human Rights Committee,[115] where members commit to acting in a manner consistent with GNI Principles.

GNI members are independently assessed every two years on their progress in implementing GNI's principles.[116] The purpose of the assessment is to ensure that members are making a good faith effort to implement the principles over time.[117] An assessment of a GNI member includes both a company Process Review and a review of specific Case Studies.[118] The Process Review examines a company's systems, policies, and procedures to implement the GNI principles.[119] The Case Study would relate to the company's relevant policies from the Process Review and show whether and how the member implemented the GNI principles in practice.[120] The assessment process remains confidential and reports that are presented to the public are aggregated and anonymized.[121]

If it is found that there is a compliance issue or pattern of problems from a GNI member, then the member will have to develop and implement a corrective action plan to remedy the identified problems and report the plan to GNI's Executive Director.[122] GNI's Executive Director and/or relevant GNI staff or members may be involved during the corrective action process to ensure that a solution is found.[123] GNI publicly reports on the outcome of the assessments each year, highlighting its decisions with non-compliant companies.[124]

---

[114] *See The Operation of the GNI Principles When Local Law Conflicts with Internationally Recognized Human Rights,* GLOB. NETWORK INITIATIVE, https://globalnetworkinitiative.org/operating-difficult-jurisdictions/ (last visited Jan. 23, 2022).
[115] *See generally* International Covenant on Civil and Political Rights, *supra* note 104.
[116] *See Company Assessment,* GLOB. NETWORK INITIATIVE, https://globalnetworkinitiative.org/company-assessments/ (last visited Jan. 23, 2022).
[117] *Id.*
[118] *Id.*
[119] *Id.*
[120] *Id.*
[121] *Id.*
[122] *See* GLOB. NETWORK INITIATIVE, GNI ASSESSMENT TOOLKIT 50 (Oct. 2021), https://globalnetworkinitiative.org/wp-content/uploads/2021/11/AT2021.pdf.
[123] *Id.*
[124] *Id.*

Self-regulatory third-party groups like the NAI and GNI face criticisms. First, while companies that are members of these groups face the threat of being reprimanded if they violate the group's principles, it appears this penalty may remain anonymous to the public.[125] Since naming the company is not required, the public can go unaware that the company's peers disapprove of its privacy measures. Second, GNI's assessments may take too long. Two years in between check-ins to review company's good-faith efforts in implementing its principles seems like a slow and plodding process.[126] Third, for a self-regulatory group to be effective, it should include most of its industry members. If just a fraction of an industry is participating, then many consumers who engage with the rest of the same industry are not subject to similar protections that the self-regulatory group imposes. Fourth, membership of the self-regulatory groups appears to be vacillating. In 2000, the NAI had twelve members, which then fluctuated down to two in 2002-03.[127] Companies were able to end memberships without consequence. The numbers of members went back up after NAI added an "Associate Membership" where companies could become NAI members without full compliance.[128]

3. Third-Party "Trust" Authorities

In May 2000, the FTC submitted a report to Congress called *Privacy Online: Fair Information Practices in the Electronic Marketplace* that outlined a tool that private industries could use for self-regulation.[129] This early tool, known as TRUSTe, was the first online privacy seal program.[130] This program allowed companies to display TRUSTe's privacy seal on their websites if they implemented certain fair information practices and submitted to various types of compliance monitoring.[131] The belief was that if this program was widely adopted, it would provide an efficient way to alert consumers of the company's information practices and compliance with TRUSTe's privacy program. This program appeared to be effective considering the complex website

---

[125] *See Compliance,* NAI, https://thenai.org/accountability/compliance/ (last visited Jan. 23, 2022) ("Further, the NAI may publicly name a company or the violation in the compliance report, and/or elsewhere as needed, when NAI determines that a member has engaged in a material violation of the 2020 Code of Conduct.").
[126] GLOB. NETWORK INITIATIVE, *supra* note 116.
[127] PAM DIXON, WORLD PRIV. F., THE NETWORK ADVERTISING INITIATIVE: FAILING AT CONSUMER PROTECTION AND AT SELF-REGULATION 28-30 (2007), https://www.worldprivacyforum.org/2007/11/report-nai-membership-problems-of-the-nai/.
[128] *Id.*
[129] FAIR INFORMATION PRACTICES, *supra* note 47.
[130] *Id.*
[131] *Id.*

privacy statements that inundated consumers on the Internet. These third parties could review the privacy policies on the consumers' behalf.[132] Users could trust the website's practices after viewing an icon, such as a privacy seal or watermark, indicating that the website met TRUSTe's approval and privacy requirements.[133] TRUSTe seals also assured consumers that businesses' websites followed privacy laws such as COPPA and the U.S.-EU Safe Harbor framework.[134]

This third-party development appeared as a successful method for the private industry to self-regulate. Companies seeking TRUSTe certification would provide TRUSTe access to their online properties.[135] This allowed TRUSTe to ensure that privacy statements conformed to actual practices.[136] Seal holders were also required to go through an annual recertification to ensure that compliance is continual. TRUSTe's privacy guidelines were designed with the FTC's self-regulatory guidelines in mind.[137]

However, the effectiveness of seal programs remain limited. Some critics argue that it is too easy for websites to attain a TRUSTe seal with some sites receiving approval while under an FTC investigation.[138] Few certifications have been revoked since its development, perhaps indicating a lack of enforcement.[139] Next, many third-party trust authorities are paid by the same companies that they certify, indicating potential conflicts of interests.[140] Since its introduction, the amount of websites that existed a few decades ago has grown exponentially. TRUSTe's ability to maintain oversight and monitoring appears to have faltered when, in 2014, TRUSTe settled with the FTC due to inadequate oversight.[141] TRUSTe was charged with deceiving consumers for failing to conduct annual recertifications for over 1000 companies even though it states on its website that companies with its seal receive recertification annually.[142] TRUSTe was required to pay the FTC $200,000 as part of its settlement and is prohibited from making misrepresentations about

---

[132] *Id.*
[133] *Id.*
[134] *U.S.-EU Safe Harbor Framework*, FED. TRADE COMM'N, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/u.s.-eu-safe-harbor-framework (last visited May 6, 2021).
[135] BELLIA, BERMAN, FRISCHMANN & POST, *supra* note 21, at 526.
[136] *Id.*
[137] *Id.*
[138] *Id.* at 527.
[139] *Id.*
[140] *Id.*
[141] *TRUSTe Settles FTC Charges it Deceived Consumers Through Its Privacy Seal Program*, FED. TRADE COMM'N, (Nov. 17, 2014), https://www.ftc.gov/news-events/press-releases/2014/11/truste-settles-ftc-charges-it-deceived-consumers-through-its.
[142] *Id.*

its certification process timeline.[143] Additionally, TRUSTe is barred from allowing companies to misrepresent their participation in TRUSTe's privacy programs.[144]

A study conducted in 2015 analyzed whether different types of industry-led standards improved online privacy and security.[145] The study analyzed over 10,000 websites that still existed in 2015 and assessed them beginning in 2007. The study considered several factors to gauge trustworthiness such as a website's privacy policy, security, availability of contact information, privacy statements, and secure protocols on billing pages. The study compared TRUSTe certified and uncertified websites against each other. Initially, websites that had the TRUSTe seal in 2007 were rated as trustworthy but their levels decreased by 2015. The conductor of the study concluded that there is no evidence that paid certifications, like TRUSTe, improve the privacy protections for the users of websites.[146]

In 2017, nearly twenty years since its introduction, TRUSTe rebranded and changed its name to TrustArc.[147] The name change "reflect[ed] its evolution from a privacy certification company into a global provider of technology-powered privacy compliance and risk management solutions."[148] Today, instead of solely offering certifications, TrustArc now offers technology solutions and consulting services to its clients.[149]

D. Contemporaneous Example

Clearly, self-regulation in the private industry has evolved in the past thirty years thanks to the influence of the FTC. Several attempts have been made by trade associations and third-party trust authorities to protect consumer privacy. A contemporaneous example of an attempt at self-regulation is Facebook's newly developed Oversight Board.[150] The

---

[143] *Id.*
[144] *Id.*
[145] Siona Listokin, *Industry Self-Regulation of Consumer Data Privacy and Security*, 32 J. MARSHALL J. INFO. TECH. & PRIV. L. 15, 15 (2015).
[146] *See id.* at 26.
[147] Press Release, TRUSTARC, TRUSTe Transforms to TrustArc (Jun. 7, 2017) https://trustarc.com/truste-transforms-to-trustarc/.
[148] *Id.*
[149] *Id.*
[150] Andrew Hutchinson, *Facebook Outlines Content Review Board Process, Which Will Provide Independent Case Assessments*, SOC. MEDIA TODAY (Jan. 30, 2020), https://www.socialmediatoday.com/news/facebook-outlines-content-review-board-process-which-will-provide-independ/571342/.

idea for Facebook's Oversight Board (FOB) was developed in 2018.[151] In 2019, forty-three lawyers, academics, and media experts gathered to draft the proposal and charter for FOB.[152] FOB has colloquially been called Facebook's Supreme Court.[153] In 2020, the Oversight Board officially formed and began operations. FOB was designed to focus on the most challenging issues for Facebook, including hate speech, harassment, and protecting people's safety and privacy.[154] Recognizing the influence that Facebook has on people's lives, and that social media has become a lifeline for people during the COVID-19 global pandemic, Facebook created the Oversight Board to review its decisions.[155]

Like a quasi-judicial system where parties can appeal a decided case to a Court of Appeals or Supreme Court, users can make appeals to the Oversight Board on decisions made by Facebook and Instagram.[156] The Oversight Board evaluates the submitted cases but has a defined criterion for which cases it reviews in depth.[157] FOB will select cases that are "difficult, significant and globally relevant [and] can inform future policy."[158] A panel of members of the Oversight Board will be assigned to review the case. The assigned panel will "deliberate the case and make a decision based on all the information provided by the person who submitted by the appeal, by Facebook and by any experts called upon to provide further context."[159] The Oversight Board will provide a written explanation of its decision, which is available for the public to read.[160] The Oversight Board's decisions are binding, which means Facebook is

---

[151] *See* Cecilia Kang, *What is the Facebook Oversight Board?,* N.Y. TIMES (May 5, 2021), https://www.nytimes.com/2021/05/05/technology/What-Is-the-Facebook-Oversight-Board.html.
[152] *See* Kate Klonick, *Inside the Making of Facebook's Supreme Court*, THE NEW YORKER (Feb. 12, 2021), https://www.newyorker.com/tech/annals-of-technology/inside-the-making-of-facebooks-supreme-court.
[153] *See id.*
[154] *See* Siva Vaidhyanathan, *Facebook and the Folly of Self-Regulation*, WIRED (May 9, 2020), https://www.wired.com/story/facebook-and-the-folly-of-self-regulation/.
[155] *See* Catalina Botero-Marino, Jamal Greene, Michael W. McConnell & Helle Thorning-Schmidt, *We Are a New Board Overseeing Facebook. Here's What We'll Decide*, N.Y. TIMES (May 6, 2020), https://www.nytimes.com/2020/05/06/opinion/facebook-oversight-board.html?smid=tw-nytopinion&smtyp=cur.
[156] Lakshmi Gopal, *Facebook's Oversight Board & the Rule of Law: The Importance of Being Earnest,* AM. BAR ASS'N.: BUS. L. SECTION (Oct. 12, 2021), https://businesslawtoday.org/2021/10/facebooks-oversight-board-the-rule-of-law-the-importance-of-being-earnest/#_ftn7.
[157] *Appealing Content Decisions on Facebook or Instagram*, OVERSIGHT BD., https://oversightboard.com/appeals-process/ (last visited May 6, 2021).
[158] *Id.*
[159] *Id.*
[160] *Id.*

required to implement its decision unless doing so would violate the law.[161]

The Oversight Board has stated that its decisions are free of influence from Facebook and that it is guaranteed by Facebook's structure:

> …[O]perations are funded by a $130 million trust fund that is completely independent of Facebook and cannot be revoked. Board members will serve fixed terms of three years, up to a maximum of three terms; they contract directly with the oversight board. We cannot be removed by Facebook. Through the founding bylaws of the oversight board, Facebook has committed to carrying out our decisions even though it may at times disagree […] Mark Zuckerberg, has also personally committed to this arrangement.[162]

The Oversight Board is comprised of a diverse membership, both culturally and professionally. Members are selected based on their experiences of "deliberating thoughtfully and collegially," skilled at decision-making based on set principles, and are familiar with digital content and governance.[163] Currently, FOB has twenty members who range from Nobel Peace Prize winners to constitutional law experts to human right advocates to former prime ministers.[164] Facebook's Oversight Board has been described as the "first time a private transnational company has voluntarily assigned a part of its policies to an external body like this."[165] This is not exactly true since earlier in this paper it was observed that industry trade associations have developed self-regulatory membership-based organizations that set guidelines and standards for their participants. However, FOB is groundbreaking in the sense that there is no other private company in the world that is comparable to Facebook. Facebook is its own industry. There are arguably no other members in its industry group that can set standards for it.[166]

Facebook's attempt to develop a self-regulatory governance structure has resulted in apprehension. First, commentators argue that

---

[161] *Id.*
[162] *See* Botero-Marino, Greene, McConnell & Thorning-Schmidt, *supra* note 155.
[163] *Our Commitment*, OVERSIGHT BD., https://oversightboard.com/meet-the-board/ (last visited May 6, 2021).
[164] *Id.*
[165] Vaidhyanathan, *supra* note 154.
[166] *See id.*

Facebook lacks "democratic legitimacy."[167] The objectives that Facebook is developing for its Oversight Board are not the result of statutory or constitutional authority,[168] compared to what the FTC did for online consumers' privacy protections.[169] FOB's rules and standards were not developed by an administrative agency, elected legislature or judicial system that carries democratic legitimacy. Facebook's implementation of its Oversight Board is unilateral even though it is attempting to separate itself from the Board.[170]

Second, there are concerns that Facebook is using the Oversight Board to define its duties towards the public.[171] Facebook is once again not using standards or guidelines outlined by an administrative agency or international law in developing its governance.[172] It is developing its own norms that might be acceptable to most of its users. As a company that touches countless lives daily, perhaps there are certain duties that Facebook is intentionally leaving out. Additionally, the Oversight Board is unable to generate general standards for Facebook since the FOB will only be reviewing worst-case scenarios one-by-one. The process will be slow and narrow before any general standards are set for Facebook.

Another criticism is that FOB is stacked with a disproportionate number of Americans.[173] Five out of the twenty board members are Americans. These individuals may view cases through a lens of U.S. history and conflicts. They also might not possess a deep understanding of how social media operates in different areas of the world. There is only one FOB member from India, a country that has more Facebook users than any other country in the world.[174] India is a diverse country that is home to more than twenty-two major languages and 700 dialects.[175] This challenges the notion whether the FOB is readily equipped to handle complex problems relating to Facebook in India.[176]

FOB does present some of the typical benefits that self-regulation provides to private companies. The Oversight Board is comprised of experts who can provide informed and targeted intervention, flexibility, responsiveness, and greater compliance.[177] While Facebook makes its

---

[167] Chinmayi Arun, *The Facebook Oversight Board: An Experiment in Self-Regulation,* JUST SEC. (May 6, 2020), https://www.justsecurity.org/70021/the-facebook-oversight-board-an-experiment-in-self-regulation/.
[168] *Id.*
[169] *See* Federal Trade Commission Act, 15 U.S.C. §5(a) ("unfair or deceptive acts" language used to enforce penalties by the FTC for privacy violations).
[170] Klonick, *supra* note 152.
[171] Arun, *supra* note 167.
[172] *Id.*
[173] Vaidhyanathan, *supra* note 154.
[174] *See id.*
[175] *See id.*
[176] *Id.*
[177] Arun, *supra* note 167.

own rules, like many private companies, it may be more willing to comply with decisions made by its Oversight Board rather than from a governmental counterpart. Facebook can also speedily respond to the decisions made by FOB.[178] For example, Facebook was able to respond quickly to issues of disinformation that resulted from COVID-19. In contrast, it can be difficult for government institutions to respond as quickly.[179]

Moreover, the Oversight Board has repeatedly emphasized that it is independent in thought and judgment of Facebook. Therefore, Facebook is answerable to a separate body that may help Facebook to regain public trust after the events from recent years.[180] Further observance is required of the recently created Oversight Board to ensure its accountability.

III. NOW WHAT?

For the last thirty years, consumer privacy protections have been managed by self-regulation in combination with various statutes and agency guidance. While self-regulation was heavily idealized in the early 1990s and was recommended by the FTC, it has proven itself to be inadequate in the current Internet landscape. The online marketplace has expanded since the FTC first introduced Fair Information Practices (FIPs) in 1998 and while industries have tried to implement FIPs into their own forms of self-regulation, entities such as NAI and Third-Party "Trust" Authorities have fallen short.

Genuine self-regulation by the private industry also does not appear to truly exist since the FTC is heavily entangled with self-regulation. The FTC has been involved since the beginning of the development of various self-regulation regimes. The FTC's introduction of FIPs, its investigations into data privacy claims, and initial support for Third-Party Trust authorities established a set of directives for the private industry to follow.

The Electronic Privacy Information Center (EPIC) has expressed disappointment in self-regulation as early as 2005.[181] In its 2005 report, *Privacy Self Regulation: A Decade of Disappointment*, EPIC criticized the length of time it has taken for privacy practices to take effect in the

---

[178] *Id.*

[179] Nick Clegg, *Combating COVID-19 Misinformation Across Our Apps*, FACEBOOK (Mar. 25, 2020), https://about.fb.com/news/2020/03/combating-covid-19-misinformation/.

[180] Sarah Feldman, *Facebook Loses the Public's Trust*, STATISTA (Dec. 14, 2018), https://www.statista.com/chart/16431/tech-company-trust/.

[181] *See* Chris Jay Hoofnagle, *Privacy Self Regulation: A Decade of Disappointment*, ELEC. PRIV. INFO. CTR. (Mar. 4, 2005), https://epic.org/reports/decadedisappoint.html.

online marketplace.[182] EPIC assessed the members of Direct Marketing Association, a self-regulatory body that is similar to the NAI, and found that only eight out of its 76 members kept privacy policies on their websites.[183] EPIC demanded more enforcement by the FTC and called the FTC's hands-off approach as delaying the adoption of substantive legal protection for privacy.[184] EPIC stated that the Commission's approval of entities such as the NAI and TRUSTe allows businesses to continue collecting personal information without providing meaningful privacy protection.[185]

In 2005, EPIC reported that "online collection of information is more pervasive, more invasive, and just as unaccountable as ever—and increasingly, the public is anesthetized to it."[186] Now in 2022, as the FTC continues its hands-off approach, information collection is still pervasive and invasive, and the public is still unaware to violations of its privacy. However, if the FTC and Congress take substantive action industries can implement fairer practices to protect online consumers. Immediate action depends on various factors aligning, including general congressional approval of the FTC's current authority as a privacy enforcer and rare consensus amongst Congress.

This final section of the paper moves on to briefly consider solutions to increasing privacy protections in the self-regulatory era that currently exists.

A. An Aggressive Federal Trade Commission

A potential solution to the current self-regulatory regime for consumer privacy is increased FTC enforcement. Currently, the FTC's approach to consumer privacy protections is not aggressive. Any case that the FTC takes on when investigating privacy claims usually ends in a settlement.[187] The FTC has also only provided guidelines for the private industry to implement. These guidelines, such as the FIPs, have been described as vague with the private industry bending the rules to its benefit.[188] The FTC can strengthen consumer protection in two ways: a more aggressive approach or codified authority by Congress.

---

[182] *See id.*
[183] *See id.*
[184] *See id.*
[185] *Id.*
[186] *Id.* at 5.
[187] *New Common Law of Privacy*, *supra* note 34, at 588.
[188] Fred H. Cate, *The Failure of Fair Information Practice Principles, in* CONSUMER PROTECTION IN THE AGE OF THE INFORMATION ECONOMY 343, 356 (Jane K. Winn ed., 2006), https://www.ftc.gov/system/files/documents/public_comments/2018/12/ftc-2018-0098-d-0036-163372.pdf (describing the Fair Information Principles as vague).

An increased aggressive approach by the FTC would mean heavier enforcement when legally challenging the privacy practices of companies. The Commission should take "more ground-breaking and norm-nudging cases" that do not end up dropped or settled.[189] The FTC has been described as risk-averse and fearful of blowback from Congress.[190] Bad press in the 1970s resulted in the FTC's apprehension of congressional disapproval.[191] However, the climate is different now. Cybersecurity is a top legal issue today and the FTC has established its presence as an enforcement agency. Many industries look to the FTC as a developer of privacy common-law. By refusing to settle claims and taking on increasingly challenging cases, the FTC could develop new norms surrounding the protection of consumers' privacy. This new standard would demonstrate to companies who look to the FTC for guidance that the current self-regulatory regime is changing.

Another way to strengthen the FTC's enforcement is to increase its budget. The FTC is constrained by resources with a budget of just over $300 million.[192] As a small agency with a broad mission in competition and consumer protection, only about 50 of its 1,100 employees are tasked with privacy.[193] Therefore, the FTC's 50 employees who take on all the U.S. companies' privacy practices are under severe resource constraints. They require increased resources to effectively tackle privacy challenges to send a clear message to companies. On average, the FTC announces 15-20 Section 5 enforcement settlements per year.[194] Some small companies may think they are immune from the FTC's attention if they conduct privacy violations because they believe themselves too small and inconsequential. With increased funding, the FTC can hire more staff to focus on privacy. With more people involved in the FTC's privacy work, the Commission can increase the number of cases it takes on. With an increased number of cases, this can result in a deterrent effect for both small and large companies—small companies who think they are

---

[189] *See* CHRIS JAY HOOFNAGLE, WOODY HARTZOG & DANIEL J. SOLOVE*, The FTC Can Rise to the Privacy Challenge, but Not Without Help from Congress*, LAWFARE (Aug. 9, 2019), https://www.lawfareblog.com/ftc-can-rise-privacy-challenge-not-without-help-congress.

[190] *Id.*

[191] *See* CHRIS HOOFNAGLE, *KidVid in Context*, TECH. ACADS. POL. (June 8, 2018), https://hoofnagle.berkeley.edu/wp-content/uploads/2018/06/kidvid_in_context.pdf. (The FTC attempted to regulate problematic advertising to children, but its campaign was found to be ineffective, poorly conceived, and over-reaching).

[192] FED. TRADE COMM'N, FISCAL YEAR 2021 CONGRESSIONAL BUDGET JUSTIFICATION 46 (2020), https://www.ftc.gov/system/files/documents/reports/fy-2021-congressional-budget-justification/fy_2021_cbj_final.pdf.

[193] HOOFNAGLE, HARTZOG & SOLOVE*, supra* note 189.

[194] *Id.*

invisible and large companies who realize they might be made into the next example.[195]

Congress should codify the FTC's authority to set standards for consumer privacy protections. The Commission has already been enforcing privacy protections under the authority of Section 5 of the FTC Act. They can do so under their mission to prevent unfair and deceptive acts affecting consumers. Additionally, the FTC has the authority to issue regulations and enforce COPPA, so the FTC already has the experience and the existing structure. Through a body of common law, the FTC has established itself as the leading agency protecting Americans' online privacy.[196] With Congress's support to fully enforce and challenge privacy harms, the FTC does not have to selectively pick and choose what cases it takes on out of fear of upsetting Congress. The FTC can boldly set the norms for companies' treatment towards consumer privacy.

The National Institute of Standards and Technology (NIST) can serve a role in aiding the FTC by engaging their National Cybersecurity Center of Excellence (NCCoE). The NCCoE works with industry organizations, government agencies, and academic institutions to address pressing cybersecurity issues.[197] Congress can support the NIST and FTC by defining their roles.[198] NIST can have authority to approve inventions that may have components that are susceptible to data hacks and cybersecurity threats just as the FDA approves products before they go on the market.

B. Comprehensive Federal Data Privacy

Congressional enactment of comprehensive privacy legislation would increase consumer privacy protections. Dating back as far as 1998, the FTC has recommended that Congress enact legislation to ensure adequate protection of consumers' privacy online.[199] Initially, the Commission's recommendations focused on children's privacy online.[200] Then starting in 2000, the Commission called upon Congress for the

---

[195] *See id.*

[196] *New Common Law of Privacy*, *supra* note 34, at 676 ("The FTC has risen to act as a kind of data protection authority in the United States. Despite having limited jurisdiction and limited resources, the FTC has created a body of common law doctrines through complaints, consent decrees, and various reports and other materials.").

[197] *About the Center*, NAT'L CYBERSECURITY CTR. OF EXCELLENCE, https://www.nccoe.nist.gov/about-the-center (last visited May 6, 2021).

[198] Andrea Arias, *The NIST Cybersecurity Framework and the FTC*, FED. TRADE COMM'N (Aug. 31, 2016, 2:34 PM), https://www.ftc.gov/news-events/blogs/business-blog/2016/08/nist-cybersecurity-framework-ftc.

[199] *See* PRIVACY ONLINE, *supra* note 31, at 42.

[200] *Id.*

protection of all online users who are not protected by the COPPA.[201] In this 2000 report, the Commission urged the private industry to continue strengthening its self-regulatory approach for consumer privacy protection even under new privacy legislation.[202]

As recently as 2020, the FTC has requested in front of both the House and Senate that Congress enact privacy and data security legislation.[203] This legislation would be enforceable by the FTC and would have authority granted by the Administrative Procedure Act.[204] While the four sitting commissioners of the Federal trade Commission are split evenly along party lines, they all agree that the best solution to protect consumer digital privacy is for Congress to enact a digital privacy law.[205] Commissioner Noah Joshua Phillips believes data security legislation is a critical step for Congress to protect consumer privacy.[206] Commissioner Phillips also believes this legislation should be based on harms that Congress agrees warrant a remedy, and that tools like penalties and rulemaking should be calibrated carefully to address those harms.[207] It is noteworthy that the FTC has called for federal privacy legislation from Congress for almost thirty years now with no results thus far.

The Commission has recommended that proposed privacy legislation set forth a basic level of privacy protection for all visitors to consumer-oriented commercial websites.[208] This legislation would set out the necessary standards of practice governing the collection of information online. Legislation would also provide the FTC with the authority to promulgate more detailed standards pursuant to the Administrative Procedure Act, including authority to enforce those standards.[209] All consumer-oriented commercial websites that collect personal identifying information from or about consumers online would be required to comply with the five widely accepted fair information

---

[201] *Id.*
[202] *Protecting Consumers and Fostering Competition in the 21st Century: Hearing Before the Subcomm. on Fin. Servs. and Gen. Governance of the H. Comm. on Appropriations*, 116th Cong. (2019) (statement of Joseph Simons, Chairman, Fed. Trade Comm'n), https://www.ftc.gov/system/files/documents/public_statements/1545285/appropriations_committee_testimony_092519.pdf [hereinafter *Protecting Consumers*].
[203] *See id.*
[204] *See id.*
[205] Lauren Feiner, *FTC Commissioners Agree They Should Act to Protect Consumer Privacy if Congress Doesn't*, CNBC (Apr. 20, 2021) https://www.cnbc.com/2021/04/20/ftc-commissioners-agree-they-should-protect-consumer-privacy.html.
[206] *See Protecting Consumers*, *supra* note 202, at 8 n.11.
[207] *See id.*
[208] *See* FAIR INFORMATION PRACTICES, *supra* note 47, at iii.
[209] *Id.*

practices: (1) Notice, (2) Choice, (3) Access, (4) Security, and (5) Enforcement.[210]

The FTC has expressed a desire for stakeholders to be involved in the development of privacy legislation.[211] This would include the private industry and consumers actively participating in the development of legislative regulations.

While the FTC has called on Congress for legislation, it has also called on industries to continue with self-regulation.[212] Private industry self-regulation as an adjunct to government regulation seems promising. The Children's Online Privacy Protection Act (COPPA) can serve as a model for implementing legislation into the existing self-regulatory framework. COPPA's Safe-Harbor Program allows industry groups to submit to the FTC self-regulatory guidelines that implement the protections of COPPA.[213] This appears to shift some of the costs of regulation to the private sector, while ensuring that all industry participants are subject to the minimum standards outlined by COPPA. This approach provides some of the benefits that comes from self-regulation: flexibility and the superior industry knowledge.[214] COPPA's Safe Harbor approach can be implemented in potential privacy legislation shifting costs and efforts onto the private industry.

Perhaps the realization for privacy legislation is not far off. In 2015, the Obama administration proposed a broad consumer data privacy bill.[215] The proposed bill intended to provide Americans with more control over the personal information that is collected by online companies.[216] Various privacy scholars and organizations analyzed the White House framework.[217] Some welcomed the initiative of the White House for tackling pertinent issues, while others criticized the draft claiming it missed the mark.[218] The proposal called on Congress to enact legislation to protect Americans' personal information. Then in 2019,

---

[210] *See* PRIVACY ONLINE, *supra* note 31, at 7.
[211] *See* PROTECTING CONSUMER PRIVACY, *supra* note 62, at 2 (FTC has hosted dozens of roundtable discussions engaging stakeholders where they explore privacy implications such as privacy legislation and self-regulatory regimes.).
[212] *See* SELF-REGULATORY PRINCIPLES, *supra* note 61, at 1.
[213] *COPPA Safe Harbor Program,* FED. TRADE COMM'N, https://www.ftc.gov/safe-harbor-program (last visited May 6, 2021).
[214] *See* Campbell, *supra* note 2.
[215] OBAMA WHITE HOUSE ARCHIVES, ADMINISTRATION DISCUSSION DRAFT: CONSUMER PRIVACY BILL OF RIGHTS ACT OF 2015 (2015), https://obamawhitehouse.archives.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf.
[216] *See* Natasha Singer, *White House Proposes Broad Consumer Data Privacy Bill*, N.Y. TIMES (Feb. 27, 2015), https://www.nytimes.com/2015/02/28/business/white-house-proposes-broad-consumer-data-privacy-bill.html.
[217] *See generally id.*
[218] *Id.*

under a different administration, Congress came to a rare consensus desiring a national privacy law.[219] Senator Roger Wicker, the Senate Commerce Committee Chair, stated that several meetings and discussions were taking place amongst congressional members.[220] There were discussions of the need for a comprehensive federal data privacy law that would unify the inconsistent and varied laws that exists across the states.[221] Senator Wicker stated that the Senate was making good progress on efforts to develop the legislation.

However, legislation has yet to be produced and is likely to be delayed even further by the COVID-19 pandemic. There appears to be no further progress made since Senator Wicker's statements in 2019.

CONCLUSION

The current framework of self-regulation by private industry exists thanks to the FTC's guidance and the response by private companies to meet the FTC's principles. However, online consumers cannot rely solely upon the private industry to self-regulate to ensure their privacy. To ensure the protection of online consumers, the FTC should take a more aggressive approach when challenging private companies who violate consumer privacy. Online consumers also need congressional intervention through legislation to guarantee at least a minimal, enforceable privacy right. The standards that private industry has developed to guide its self-regulation provides much of the basic body of safeguards consumers need. Combined with congressional legislation or an aggressive FTC, this can bolster online consumers' confidence in the online marketplace.

---

[219] *See* David McCabe, *Congress and Trump Agreed They Want a National Privacy Law. It Is Nowhere in Sight,* N.Y. TIMES (Oct. 1, 2019), https://www.nytimes.com/2019/10/01/technology/national-privacy-law.html.
[220] *Id.*
[221] *Id.*