Volume 124 | Issue 1 Article 1

9-9-2021

Data Privacy Issues in West Virginia: An Overview

Jena Martin
West Virginia University College of Law, jena.martin@mail.wvu.edu

DATA PRIVACY ISSUES IN WEST VIRGINIA: AN OVERVIEW

Jena Martin+

I. WHAT'S AT STAKE 3
II. THE CURRENT REGULATORY FRAMEWORK 4
A. The Stakeholders Involved 4
B. Recent Federal Initiatives 5
C. The Current State Landscape 5
III. CONSIDERATIONS FOR WEST VIRGINIA 7
A. Summary of Initial Survey 8
B. Summary of Focus Group Sessions 9
C. Focus Group Recommendations 10
IV. RECOMMENDATIONS & PROPOSED BEST PRACTICES 11
A. General Principles for Developing a Regulatory Framework 11
B. Implications for Practitioners in the Field 15
V. CONCLUSION 17

"We now live in an age of personal information. Such personal information drives the economy and can be used to influence policy, our elections, our identities,' and even our moods."[1]

This essay is about data privacy in West Virginia. However, many of the issues that affect West Virginians also affect people around the country and the world. As such, it's also an essay about the state of data privacy today and the current challenges that affect people nationally and globally. West Virginia serves as an important focal point for several reasons. First, West Virginia has been in the national news within the last few years as a bell-weather for various

+ Professor of Law, West Virginia University. This essay is adapted from a larger white paper about data privacy. The paper was drafted with the help of several WVU students: Cheryl Brown, Allyson Burrowes, Trista Campbell, Jeremy Cook, Jayda Guidry, Shawn Hogbin, Ashton Meyers, and Julia Pirillo. The references to "we" and "our" in this essay are an acknowledgement of their significant contributions to that project. In addition, Shawn Hogbin and Jonathan Marshall deserve a special thank you for their incredibly helpful comments on this essay. Finally, I owe a deep debt of gratitude to the editors of the West Virginia Law Review Online who provided vital insight and commentary that made this essay better.

[1] Neil Richards, *Why Data Privacy Law is (Mostly) Constitutional*, 56 WILLIAM & MARY L. REV. 1501, 1504 (2015).

issues affecting the nation.[2] The push back[3] from what is often one-dimensional national coverage of these issues[4] has, in turn, challenged people to move beyond stereotypical assessments of the state and engage in a more nuanced analysis of West Virginia in particular and Appalachia in general.[5] Second, because of West Virginia's topography, the state often lags beyond the nation in its broadband access.[6] While this creates difficulties for the state's current residents, it also presents an opportunity for legislators, policymakers, and practitioners to proactively address issues of data privacy at this nascent stage. Taking time to examine these issues thoughtfully now can allow us to develop useful jurisprudence, insightful commentary, and comprehensive laws that will better serve the citizens of our state for years to come.

This essay proceeds as follows. Part one provides a general overview of the current issues involving data privacy. Part two discusses the current legislative framework and the larger gaps in data privacy law. Part three summarizes the key takeaways based on responses to a survey and focus groups sessions conducted in West Virginia in 2019. Finally, part four provides ten general principles that policymakers and legislatures should consider when crafting data privacy frameworks before examining how the current state of data privacy implicates the work of practicing attorneys in West Virginia. Many of the themes and issues discussed in this essay were part of a multi-year study for the Center for Consumer Law and Education, a joint initiative of West Virginia University and Marshall University. The culmination of this study resulted in a white paper that provides a comprehensive analysis regarding how the issues of

---

[2] For instance, in the wake of the election cycles over the last few years, commentators have been focusing on West Virginia's voting patterns as a measure of the things that could affect the nation at large. *See, e.g.*, Emily Metzger, *U.S. "Flyover Country" Sends Election Signal*, NEWS DECODER (May 19, 2016), https://news-decoder.com/u-s-flyover-country-sends-election-signal/ (discussing the results from West Virginia's exit polls during the primary election season that showed that many West Virginians who voted for Bernie Sanders in the primary said they would vote for Donald Trump if Bernie Sanders failed to secure the Democratic nomination. Yet, much of the media expressed shock when six months later, Donald Trump secured the presidency).

[3] For instance, in her book *What You Are Getting Wrong About Appalachia*, Elizabeth Catte documents the recent rise in national fascination with the region and how it is often portrayed from a lens of "othering," i.e., examining residents of the state as if they were not really a part of the nation. *See generally* ELIZABETH CATTE, WHAT YOU ARE GETTING WRONG ABOUT APPALACHIA (2018).

[4] *See id.* at 22–35 (discussing the rise of "Welcome to Trump Country" pieces often published in national newspapers during Donald Trump's campaign and presidency).

[5] *See, e.g.*, NICHOLAS STUMP, REMAKING APPALACHIA: ECOSOCIALISM, ECOFEMINISM, AND LAW (2021) (offering an ecofeminist critique of the West Virginia legal framework).

[6] Rusty Marks, *Expanded Broadband Council Begins Internet Speed Survey*, STATE JOURNAL, (Oct. 30, 2017), https://www.wvnews.com/statejournal/expanded-broadband-council-begins-internet-speed-survey/article_185086e3-395d-59e2-998f-599db2632132.html (discussing WV's study and support for broadband access).

data privacy affect not just West Virginians but also people around the country and the world.[7]

I. WHAT'S AT STAKE

One of the biggest changes that impacted privacy in the last few decades has been businesses' ability to collect, keep, and utilize data digitally. While the data records of individuals have been requested and used by corporations for decades, the amount of data that a company could keep indefinitely was limited by the sheer physical space needed to house all the information. The volume of documents that needed to be stored resulted in corporations destroying files and developing document retention practices to delete older information. In addition, before the use of computer programs, any information that a corporation wanted to collate and categorize had to be done by a human being–usually by hand. For instance, if an insurance company wanted to check historical data on a claimant, an employee for the company would have to research what, if any, claims a claimant had previously filed and spend some time checking to make sure that the claims were filed by the same individual (and not just two people with the same names). The company would then have to request the relevant box (or boxes) from whatever storage facility held that information. Then, depending on how many boxes of data the claim generated, the individual claims adjuster would have to go through all that information (almost certainly paper files) to see if there was anything relevant that would impact the current claim. With so much time and effort involved, many companies might have rightly concluded that whatever information an adjuster might glean was not worth the time and expense to get. And so, the data would remain within the domain of that initial claim and that initial claim only.

Now, however, documents that previously required thousands of square feet of space to store can be placed on a storage card that is the size of a thumb.[8] Similarly, data that once required thousands of hours to organize, collate, and sort, can now all be managed with the press of the button that often activates a machine-learning algorithm. The effects of this switch are profound. In theory, there are few limits to the amount of information a business can acquire about you, leading some scholars to proclaim that many businesses know more about you than you know about yourself.[9]

In addition, the rise of machine learning formulas and the use of algorithms to replace individual decision-making has led to several issues that

---

[7] *See* JENA MARTIN, DATA PRIVACY ISSUES IN WEST VIRGINIA AND BEYOND: A COMPREHENSIVE OVERVIEW (2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3873301.

[8] As mentioned earlier, minimizing the space requirements for documents also allows corporations to keep records significantly longer than they otherwise could.

[9] Lori Andrews, *His Profit, Your Problem*, N.Y. DAILY NEWS (May 20, 2012), https://www.kentlaw.iit.edu/sites/ck/files/public/institutes-centers/islat/His-Profit-Your-Problem.pdf.

impact data privacy in both the collection and use of data. For instance, AI algorithms can perform "data mining" by processing data from an almost unlimited number of sources, including user interaction with websites and email accounts, social media, location data on smartphones, online financial activity, data sensors, and data entry by humans into databases. Collecting this much data without either (1) informing the targeted person (and giving them the chance to correct inaccuracies) or (2) meaningful human oversight and "spot checks" of the data's accuracy could lead to significant misinformation being generated. In addition, the algorithm may be asked to provide a recommended 'best' course of action (or choice) for a new piece of data given all the previous data it has 'seen.' A business can choose to follow this choice and charge higher interest rates and insurance premiums, hire certain candidates for employment, or terminate employment – all based on results from algorithmic formulas. They can also follow the formula to determine where resources should be utilized and where they should be withheld. Many businesses who choose to deploy these tactics do so in the name of efficiency and cost-reduction, but often without realizing the biases that may be programmed into the algorithm as well.

II. THE CURRENT REGULATORY FRAMEWORK

The current regulatory framework amounts to a patchwork of cases, laws, players, and issues that cut across every industry. Part of the challenge for practitioners and policymakers in the field is this vast interconnectedness between the numerous stakeholders involved in data privacy and the amorphous nature of the laws that either protect or regulate them. While we provide an extensive analysis of all the different players and regulatory structures in our white paper, this essay highlights a few major influences.

A. The Stakeholders Involved

In addition to the consumer, who is usually the end-user (and, increasingly these days, the profit-generator for businesses involved in data collection), there are many companies involved in the collection and use of an individual's data. Some are visible—for instance, the Big Tech companies such as Amazon, Apple, Facebook and Google—while others are largely invisible, such as data brokers,[10] insurance companies, and healthcare providers. For some of these stakeholders (i.e., insurance companies and healthcare providers), existing laws are in place to regulate some of what these businesses do.[11]

---

[10] As we note in the white paper: "Data brokers obtain consumer information directly and indirectly and then compile that data into data sets for each individual. Data brokers then sell the consumer information to companies, individuals, and other data brokers. Most people don't know that data brokers exist or who they are because these brokers have an indirect relationship with the consumers from whom they obtain information." MARTIN, *supra* note 7, at 36.

[11] *See*, *e.g.*, *id.* at 21–61 (discussing the special issues for consideration with some of these stakeholders and the way the law falls short).

However, in many other situations, the current laws do not adequately address the new ways these companies have found to collect and use data.

B. Recent Federal Initiatives

There have been calls for the federal government to enact a comprehensive national law that governs data privacy.[12] While these calls have accelerated in recent years (and resulted in two bills being proposed in the last legislative session), no federal law has been passed.[13] As such, the Federal Trade Commission (FTC) has stepped in to fill the gap caused by a lack of legislation. Specifically, the FTC is the primary[14] federal agency examining data privacy issues, using its authority under Section 5 of the FTC Act to do so.[15] The agency has used two legal theories to advance its arguments: (1) that the relevant company's actions concerning data privacy amounted to fraud and (2) that the relevant corporation's conduct amounted to an unfair practice.[16]

C. The Current State Landscape

There has been a range of reactions amongst the states regarding how each is addressing data privacy issues. Most of the momentum has been around a push for state legislators to pass laws for increased data privacy protection.[17]However, in some states, courts have been actively involved in shaping potential remedies for alleged data privacy violations. This is consistent with the general types of remedies consumers currently have access to, namely: civil damages (arising from violations of common law torts), statutory damages (stemming from violations of statutory rights), and administrative remedies (for violations of federal and state rules and regulations). There are challenges with each type of claim. For instance, for those consumers wishing to access the courts, the current legal theories that have (or can be used) were originally developed before the rise of big data. As such, the current causes of actions (those that sound in contract or sound in tort) can be stymied. As one researcher

---

12 *See* Ira Rubinstein, *Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes*, 6 I/S: J.L. & POL'Y FOR INFO. SOC'Y 355, 355–59 (2011).

13 Angelique Carson, *Data Privacy Laws: What You Need to Know in 2021*, OSANO (July 20, 2021), https://www.osano.com/articles/data-privacy-laws.

14 In a recent keynote address Rebeca Kelly Slaughter, the recently appointed Chair of the FTC, has stated that issues surrounding data privacy are one of her agency's top priorities. *See* Future of Privacy, *Privacy Papers for Policymakers 2021*, YOUTUBE (Feb. 12, 2021), https://www.youtube.com/watch?v=DTjA7SgjKhw.

15 *See* Fara Soubouti, *Data Privacy and the Financial Service Industry: A Federal Approach to Consumer Protection*, 24 N.C. BANKING INST. 527, 543, (2020).

16 For a discussion of the FTC's role in this area, see Michael D. Simpson, Comment, *All Your Data Are Belong to Us: Consumer Data Breach Rights and Remedies in an Electronic Exchange Economy*, 87 U. COLO. L. REV. 669, 692–96 (2016).

17 Carson, *supra* note 13.

noted, "with data being transferred through multiple relationships, it is difficult for courts to determine who is obligated to whom. Therefore, the lack of traceability in data breach cases can create an almost insurmountable burden of proof for plaintiffs because privity can potentially exist between multiple relationships."[18]

To some extent, each state in the U.S. has been working to address data privacy concerns. For instance, all 50 states have passed laws that require businesses to notify individuals if the corporation has been affected by a data breach.[19] Many of these laws pre-dated the era of big data. There is also a patchwork of state laws regulating the collection of information by individuals. Finally, a small number of states currently regulate data brokers. For instance, in 2019, Vermont passed a law requiring data brokers to register with the state and explain whether consumers can opt out of data collection.[20] In addition, judicial opinions in various states around the nation have contributed to the development of law regarding what corporations can and cannot do with consumer data. In most jurisdictions, there is some basic protection for the various ways consumers and businesses interact around the issue of data privacy. However, many argue that states need to go beyond that and enact laws that provide a more comprehensive framework for data privacy.[21]

In addition, in July 2021, the Uniform Law Commission passed by a vote of 52-1 a proposed uniform law on data privacy.[22] Commissioners from West Virginia were among those delegates that approved the draft law. Currently, the

---

[18] Fadja Tassey, Current Topics in Internet Law Data Breach Liability, SETON HALL U.L. SCH. STUDENT SCHOLARSHIP (2018), at 4, (unpublished manuscript) https://scholarship.shu.edu/cgi/viewcontent.cgi?article=1943&context=student_scholarship.

[19] *Security Breach Notification Laws*, NAT'L CONF. OF STATE LEGISLATURES (Apr. 15, 2021), https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

[20] MARTIN, *supra* note 7, at 18.

[21] In that regard, the state of California has taken the lead with regard to this issue, enacting the California Consumer Privacy Act in 2018. The CCPA is the most comprehensive state law on the issue of data privacy. The law, which came into effect in January 2020, gives the following consumers rights: (1) the right to be aware of the types of personal information being collected, (2) the right to be aware of whether personal information is being shared and/or sold and to whom, (3) the right to opt out of having personal information sold, (4) the right to access the personal information that has been collected, (5) the right to service free of discrimination if one chooses to exercise the rights outlined above.

See CAL. CIV. CODE §§ 1798.100–1798.180 (West 2021). In addition, in July 2021, the State of Virginia became the second state to enact a comprehensive data privacy law. *See* Christopher Escobedo Hart & Colin Zick, *Virginia's New Data Privacy Law: An Uncertain Next Step for State Data Protection*, JD SUPRA (July 7, 2021), https://www.jdsupra.com/legalnews/virginia-s-new-data-privacy-law-an-8812636/.

[22] Pollyanna Sanderson, *Uniform Law Commission Finalizes Model State Privacy Law*, FUTURE PRIV. F. (July 21, 2021), https://fpf.org/blog/uniform-law-commission-finalizes-model-state-privacy-law/.

law is scheduled to be ready for circulation and adoption by state legislatures during the state sessions commencing in January 2022.[23]

While West Virginia has not enacted a comprehensive data privacy law, some statutes within the state touch on current data privacy issues. For example, West Virginia passed data breach notification legislation in 2008.[24] The law provides that any entity that has been subject to an unauthorized acquisition of a consumer's personal data must notify the affected consumer.[25] Although the statute does not provide a specific timeline, it does say that notification must occur "without unreasonable delay."[26] In addition to West Virginia's data breach law, the state has also passed a law that limits the ability of businesses to access voter registration (a significant data source for many corporations) for commercial use.[27] However, the law, in the words of one commentator, provides only "minimal statutory protection for voter data."[28]As he notes, while "[t]he state does restrict access to telephone numbers, email addresses, and identification numbers (including Social Security numbers)[,] . . . names, addresses, political parties, and registration status are all publicly available."[29]

Additionally, there is some hope that the current West Virginia case law on privacy issues could be fashioned into a framework for data privacy causes of actions. For instance, West Virginia has some extensive jurisprudence related to the collection, use, and retention of medical records that could be used as precedent (or, at a minimum, persuasive authority) for practitioners looking to craft a cause of action.[30]

III. CONSIDERATIONS FOR WEST VIRGINIA

During our multi-year study, we used surveys, focus groups, and informal conversations to check in with residents and industry representatives regarding how they view data and data privacy issues.[31] This work provides a

---

23 *Id.*

24 *See* W. VA. CODE ANN. §§ 46A-2A-101 to -105 (West 2021).

25 *Id.* § 46A-2A-102(a).

26 *Id.*

27 *Id.* § 3-2-30.

28 Charles J. Pults, *America's Data Crisis: How Public Voter Registration Data Has Exposed the American Public to Previously Unforeseen Dangers and How to Fix It*, 105 IOWA L. REV. 1363, 1375 (2020).

29 *Id.*

30 Specifically, there have been several medical protective orders filed against insurance companies regarding the retention of medical records. *See, e.g.*, State *ex rel.* State Farm Mut. Auto. Ins. Co. v. Bedell (Bedell I), 697 S.E.2d 730, 737–38 (W. Va. 2010). For a comprehensive discussion regarding the case law in this area, see MARTIN, *supra* note 7, at 48–56.

31 MARTIN, *supra* note 7, at 63–65. While data breach is the most obvious cost (in the form of identity theft fallout for the consumer and the cost to business of bolstering cybersecurity in the wake of data breaches), there are a number of other, less obvious forms of data privacy issues, including the cost to consumers for erroneous information being used to make decisions that affect

unique opportunity for the legislature to take a proactive stance using qualitative data amassed from conversations with both groups. Our discussions with each group showed that, particularly with regard to data breaches, there is a cost to both consumers and businesses.[32]

To gather information for the original white paper, we undertook two major steps. First, we conducted a survey of 500 West Virginians regarding their initial outlook and perspective on issues regarding data privacy. Then, we followed up with willing participants and conducted a series of focus groups across the state to ask more detailed questions from residents regarding their access to data. While the majority of the pool from the focus groups was drawn from the initial survey pool, we did conduct two subsequent focus groups (in Morgantown, WV) made up entirely of non-survey takers. These focus groups were unique in that they were the only focus groups that consisted entirely of individuals under the age of 30.

A. Summary of Initial Survey

The initial survey provided the breadth of the answers (quantitative research), while the subsequent focus groups allowed us to go into more depth with participants (qualitative research). Thus, the combination of the two allowed us to have both breadth and depth.

Survey responses demonstrated that many residents in West Virginia would like to see some specific remedy for data privacy harm. For instance, the strongest percentage of remedies that respondents chose were: (1) fines from government agencies and (2) free credit monitoring.[33] A large minority (33%) also indicated that they would like to see credit score freezes as part of a system of remedies.[34] This seems to indicate that many respondents were primarily concerned with identity theft issues or issues that would negatively affect their credit score.[35]

Survey results also indicate that, among initial participants, those in the under 30 age group were among the least trustful of the various entities surveyed. For instance, only 45% of people under the age of 30 trusted e-mail providers

---

them, *id.* at 25–27, the costs of biased decisions in insurance and health care decisions, *id.* at 45–48, and other more amorphous costs that come when companies collect and use consumer data without the consumers' knowledge or permission. There are also other costs that extend to the business, including the reputational harm that comes when corporations are involved in a data breach issue (or a data privacy scandal) and the cost of complying with an increasingly varied landscape of state and national legislation.

[32] This has also been echoed by researchers in this area. *See, e.g.*, Simpson, *supra* note 16, at 682–84 (discussing the cost to both industry and consumers for data breaches).

[33] LAKE RESEARCH PARTNERS, WEST VIRGINIA PRIVACY SURVEY 10 (2019) (on file with the author).

[34] *Id.*

[35] However, part of the challenge in developing a scheme is that many individuals do not even realize all the different ways that one's credit score can be damaged.

either a little or a lot – making it the lowest percentage by age group.[36] Similarly, the under 30 age group also displayed a low level of trust for cell phone carriers (41% of those surveyed stated that they had some level of distrust).[37] Those in the under 30 age group also registered the least amount of trust for online retailers, with 48% expressing some level of distrust.[38]

This low level of trust by this age group may also affect the businesses' future earning potential. For instance, according to a 2019 report, 81% of consumers have indicated that they would not use a brand that they did not trust.[39]

The survey results are similar to other surveys conducted in this area.[40] For instance, a 2019 survey conducted by the Pew Research Center found a majority of respondents feel that "data collection poses more risks than benefits."[41]

B. Summary of Focus Group Sessions

From August 2019 to February 2020, we conducted a series of focus groups to gather further information from West Virginia residents regarding their views on data privacy.[42] The focus groups met in person in the following West Virginia counties: Berkeley, Kanawha, Harrison, and Monongalia. In all, we conducted five focus group interviews.

The methodology of the focus groups (which occurred over 90 minutes) was designed to complement the quantitative research compiled from the survey

---

[36] LAKE RESEARCH PARTNERS, *supra* note 33, at 49. The next highest level of trust was displayed by those 65 and over who registered their trust levels at 47%. *Id.* at 5.

[37] *Id.* at 55.

[38] *Id.* at 61.

[39] EDELMAN, EDELMAN TRUST BAROMETER SPECIAL REPORT: IN BRANDS WE TRUST? 9 (2019), https://www.edelman.com/sites/g/files/aatuss191/files/2019-07/2019_edelman_trust_barometer_special_report_in_brands_we_trust.pdf.

[40] INTERNET SOCIETY, THE TRUST OPPORTUNITY: EXPLORING CONSUMER ATTITUDES TO THE INTERNET OF THINGS (2019), https://www.internetsociety.org/wp-content/uploads/2019/05/CI_IS_Joint_Report-EN.pdf.

[41] Brooke Auxier et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, PEW RSCH. CTR. (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/. One note of caution about the results: the information compiled for the West Virginia survey was performed by researchers at the WVU College of Law. As such, the questions, data, and methodology were not the same as what was done by other surveys.

[42] Both the initial survey and the focus groups were done with university oversight from the Office of Sponsored Research. In accordance with best practices in this area, we do not provide the names or identifying information of the focus groups' participants since we did not request (and they did not consent to) having their names included in published results. Instead, if appropriate, we provide the participants' general occupation (or major). MARTIN, *supra* note 7, at 3.

by supplementing that with qualitative research.[43] The questions began with generalized, open-ended questions designed to solicit the focus group participants' views in the most unbiased way. Then, we asked about their views on specific scenarios to clarify and challenge their positions vis-à-vis the research that we had uncovered to date.

For instance, after requesting background information regarding each participant's occupation and internet usage, the first question asked participants: what concerns (if any) they had regarding their interaction with technology. Then, for the more detailed questions, participants were given specific scenarios and asked their opinions regarding how they would react if confronted with the situation.

Participants in the Morgantown focus groups represented both the residents who fit into the 18–24 age group and those who had not previously participated in the survey. In general, their responses reflected a low level of concern for how businesses utilized their data.[44] Instead, many participants discussed the value that they believed they were obtaining from having companies access their data.[45]

C. Focus Group Recommendations

At the end of each focus group session, participants were asked to provide insight into what an ideal data privacy law would look like. Below are their recommendations.

Restrictions on Data Retention: Participants would like the law to place restrictions on who can collect sensitive data and how long they may retain the information. The law should also include specifications for how companies can and can't get rid of consumer data.

Unlimited Access to Credit Report: Participants favor free credit monitoring and believe that everyone should have total access to their credit report at all times.

Stiff Penalties and/or Fines: Participants all believed that there should be stiff penalties and/or fines per incident of data misuse or loss. Participants agreed that fines should be large enough to prevent repeat offenses (e.g., $10,000 per incident/per person). The specific amount of the fine may be based on the

---

[43] Qualitative research is not really interested in size; rather, it tries to go for depth. It tries to get a deep understanding of what people understand on an issue. It also allows us to cover a variety of situations and experiences.

[44] *See* MARTIN, *supra* note 7, at 69.

[45] For instance, one student, a marketing major, noted that she appreciated the fact that companies accessing her information could then provide her with targeted advertising that fit her needs. In addition, a second-year medical student discussed the benefits of data to advance medical research and procure life-saving measures. *Id.* at 65 n.493.

company's revenue or the CEO's salary. Some participants believed repeat offenders should be punished by fining corporate executives a percentage of their income, while others believed repeat offenders should receive criminal penalties.

Option to Opt-in/out: Participants wanted the option to opt-in or out of the collection and use of their personal data. Services that do not offer consumers this option should be prohibited from selling consumer data.

Public vs. Private Data: Participants indicated that they wanted the law to acknowledge the difference between public and private data and require companies to handle information accordingly. Specifically, services that require a log-in, two-factor authentication, or other security measures should require heightened data privacy on the premise that there is an assumption of security and confidentiality on the consumer's end.

Personal Ownership and Ability to Correct: Participants wanted personal ownership of their data. One participant suggested that there should be a website that houses the entirety of one's online information and allows for the correction of misinformation by the affected individual.

Protection of E-mails: Participants would like information exchanged via e-mail to be protected, just as letters in a mailbox.

Prohibition of Prejudicial Ad Targeting: Participants would like the law to prohibit racial or socioeconomic-based targeting. One participant suggested that to prevent prejudicial targeting, there should be some form of anonymity on purchase behavior.

IV. RECOMMENDATIONS & PROPOSED BEST PRACTICES

"*We all need reminding sometimes that if we are not paying for the product, we are the product.*"[46]

A. General Principles for Developing a Regulatory Framework

In constructing our recommendations, we have taken a deliberate approach. Rather than providing specific policy recommendations that could quickly be rendered irrelevant with the next change in technology, we have framed our recommendations as "General Principles," foundational guidelines that we hope will withstand the transformative nature of technology. In addition, we note that others (most critically, the participants of our focus groups) have

[46] Kate O'Flaherty, *Apple's Stunning iOS 14 Privacy Move: A Game Changer for All iPhone Users*, FORBES (Jan. 31, 2021, 3:59 AM), https://www.forbes.com/sites/kateoflahertyuk/2021/01/31/apples-stunning-ios-14-privacy-move-a-game-changer-for-all-iphone-users/?sh=2a0d5be7e8d3.

provided specific recommendations for a data privacy law. As such, we do not re-hash those specifics here.

General Principle #1 – **Begin with the End in Mind**

Given that technology issues seem to impact consumers of data privacy to a disproportionate degree than it does big businesses, the first recommendation starts by considering how any data privacy policy or law would affect the consumer, as the end-user, first. Will it place an onerous burden on the individual? Is it something easy to use and accessible for those affected? Initiatives that require consumers to scroll through unclear notices without a straightforward means of opting out of what businesses do with their data seem unworkable.

Beginning with the end in mind also seems to favor laws and policies that focus on data use rather than data collection, since data use is the natural ending point of data collection.[47]

General Principle #2 – Data as a Property Right

Most of the focus group participants discussed in general terms issues surrounding data with a specific ownership interest. For these focus group members, the data was *theirs*, and for many focus group members, the general theme was that this information was being taken and used without their consent. While some of the younger focus group participants did not mind sharing their data, particularly if they felt that they were receiving something in return (such as access to personalized recommendations), the key to a successful implementation of this rule is to make sure that the consumer is truly sharing or relinquishing their data of their own free will, instead of being tricked or deceived into doing it. Framing these issues as property rights underscores why authorities as diverse as the European Union and the Supreme Court of Appeals of West Virginia[48] provide heightened protection for different types of data.

General Principle #3 – Create a Centralized Agency

Tasking a central agency with overseeing data privacy has several key advantages. First, it establishes a central location where consumers, policymakers, and industry players can turn to for the definitive standard on data privacy issues. Second, allowing a government agency to focus on this issue will provide a depth of expertise at the governmental level that legislators can tap into as new issues arise.

---

[47] In our white paper we spend some time discussing the distinction between the two. *See* MARTIN, *supra* note 7, at 76.

[48] State *ex rel.* State Farm Mut. Auto. Ins. Co. v. Bedell (Bedell I), 697 S.E.2d 730, 737–38 (W. Va. 2010); *see also* MARTIN, *supra* note 7, at 20, 76.

General Principle #4 – Don't Forget the Impact of Machines

As we mentioned earlier (and expand upon significantly in our white paper), the impact of machines and machine-learning algorithms permeates every aspect of data privacy. As such, a comprehensive legal framework will need to address this head-on. This can be done in one of two ways: either more stringent measurements can be put in place on the front end to prevent machines from accessing data that can lead to discriminatory decisions, or remedies can be provided on the back end that would allow individuals to see the information that has been used in various decisions and allow them to challenge these results. Regardless, the impact of these formulas needs to be part of the conversation.

General Principle #5 – **Consider all the Players**

The network of constituents that are involved in data privacy issues is vast. While many of them (such as Big Tech companies) have garnered significant focus and attention, many more (such as data brokers) have largely escaped regulatory scrutiny. Therefore, developing a legal framework that considers *all* constituents is crucial.

General Principle #6 – Take Only What You Need

In addition to examining the *who* of data privacy, researchers have recommended that policymakers also examine the *what*. Specifically, some who write in this area have discussed being guided by the principle of data minimization.[49] Under this framework, companies would only gather the information that is central to their business.[50] Data minimization diverges from the traditional, more expansive collection methods used by corporations in the era of big data.[51] Having a more focused structure of data collection would provide some relief to consumers who are concerned with the level of detail that corporations have currently amassed about them.

General Principle #7 – Limit the Use of What You Take

---

[49] *See, e.g.*, Brittany Martin, Note, *The Unregulated Underground Market for Your Data: Providing Adequate Protections for Consumer Privacy in the Modern Era*, 105 IOWA L. REV. 865 (2020).

[50] *Id.* at 897.

[51] This indiscriminate collection of information regarding a consumer is one of the hallmarks of data collection in the last few years. Given the lower barriers to entry for the collection and storage of data, data has been transformed from a means to the end. For instance, one website identified over 200 data points that companies often collect on a consumer (including the number of surnames who are living together, your country of origin and the birth date of every member in your household). *See What Kind of Data Do Companies Collect?*, DRSOFT (Nov. 13, 2020), https://drsoft.com/2019/11/05/what-kind-of-data-do-companies-collect/.

One of the big lessons learned in the era of big data is that our uses of information can evolve at a rate directly proportional to our innovation and creativity. Thus, the data we collect today could be used in unimaginable ways in just a few years. As such, it seems unfair to permit corporations to continue using consumers' information in ways that were originally inconceivable at the time that permission was granted. Making sure the law reflects this understanding would seem to be the most equitable solution, particularly because one of the central arguments of businesses—that the data captured is central to their business model—would not apply to situations like this.

General Principle #8 – Make Privacy Easy to Understand

Research has repeatedly confirmed that corporate disclosures are rarely read and almost never understood by consumers. The language is often dense, long-winded, and varies significantly from one corporation to another. But what if we required corporations to disclose privacy issues the same way we require food companies to provide nutritional information? This is the approach that some companies, like Apple, are voluntarily taking. Having a uniform system that could be translated across companies and industries would be an easy way for consumers to make more informed decisions.[52]

General Principle #9 – Let Consumers Have Control

A key part of the work of the white paper was to hear directly from consumers about what they want. Similarly, a key facet of any legislative progress should be one where consumers have a voice in the law being shaped *and* have some control of their data at the end. It could be in the form of a Do Not Trace List (similar to Do Not Call Lists), as has been proposed by researcher Mary Kraft,[53] or it could be in more nuanced ways not yet considered. Nonetheless, keeping the focus on consumers will allow consumers to retain the choice of how their data is used.

General Principle #10 – No Need to Reinvent the Wheel[54]

---

[52] According to the Wall Street Journal, this is not a new proposal: "For years, consumer privacy advocates have pushed the idea of so-called nutrition labels for devices. Instead of telling consumers how much vitamin B or C a product has, these labels would tell the prospective purchasers how their data will be used and by whom." Cheryl W. Munk, *Imagine a Nutrition Label—for Cybersecurity*, WALL ST. J. (Dec. 8, 2020, 9:00 AM), https://www.wsj.com/articles/imagine-a-nutrition-labelfor-cybersecurity-11607436000?mod=lead_feature_below_a_pos1.

[53] Mary Kraft, Comment, *Big Data Little Privacy: Protecting Consumers' Data While Promoting Economic Growth*, 45 U. DAYTON L. REV. 97, 121 (2020).

[54] We are not alone in suggesting that policymakers rely on pre-existing models. *See, e.g.*, Cameron Kerry, *Why Protecting Privacy Is a Losing Game Today—and How to Change the Game*,

If nothing else, I hope that this essay and accompanying white paper highlights just how much work has already been done on the issue of data privacy. As such, legislators seeking to develop a data privacy framework can rely on the successes and failures of their predecessors, adjusting to adapt to the particular needs of the state.[55]

B. Implications for Practitioners in the Field

In addition to policymakers and legislators who may benefit from the guiding principles, this essay and research aim to provide initial guidance to attorneys working in the field. For instance, results from the focus groups summaries indicate that many consumers in West Virginia believe that their data should be viewed as a property right. As such, practitioners could consider formulating arguments based on this theory of the case. Although certainly a novel argument,[56] the theory could find some basis in current West Virginia case law.[57] As practicing attorneys well know, what is not achieved through legislation is often accomplished through case law; formulating a cogent argument for data as a property right could lead to key holdings in the West Virginia Supreme Court of Appeals that could then be adopted in other jurisdictions.

Another legal theory arises from West Virginia's Unfair or Deceptive Practices statute ("UDAP"), which prohibits the use of deceptive practices by entities.[58] Specifically, the law prohibits "[u]nfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce."[59] A case theory for data privacy violations based on the West Virginia UDAP has been advanced in both federal courts and tested in West Virginia state courts. Practitioners have successfully argued that the statute's language is broad enough

---

BROOKINGS INST. (July 12, 2018), https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/#_edn4.

55 For instance, we would not suggest that the state of West Virginia should develop a data privacy law akin to the GDPR. The sheer scope of the constituents the law has to cover would render that unworkable. However, looking at the work of other state legislatures to see what that they have done to address the needs of their particular stakeholders would be informative.

56 Academics, however, have considered the issue. *See*, *e.g.*, Jeffrey Ritter & Anna Mayer, *Regulating Data as Property: A New Construct for Moving Forward*, 16 DUKE L. & TECH. REV. 220, 223 (2018) (arguing for "an explicit, legal mechanism to establish, claim and transfer property rights in data").

57 *Cf.* Whitehair v. Highland Memory Gardens, Inc., 327 S.E.2d 438, 441 (W. Va. 1985) (establishing a quasi-property right in the disposition of a loved one's remains and a subsequent right to have the property treated with respect, and creating a cause of action for emotional damages for negligent mishandling of the remains); *see also* Coleman v. Sopher, 499 S.E.2d 592, 604 (W. Va. 1997) (holding same). One could see an argument using this quasi-property right within the context of data and how businesses use individuals' data.

58 W. VA. CODE ANN. § 46A-6-104 (West 2021).

59 *Id.*

to encompass misuse of a consumer's data.[60] In some instances, where an entity makes an express misrepresentation regarding data security, UDAP claims may be suitable. For instance, if an entity provides a written representation that it encrypts consumer data to protect it, and the entity fails to encrypt that data, UDAP claims potentially provide an avenue of relief. Specifically, there are several prohibited practices included in the statute that may be relevant to data privacy:

- "Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits or quantities that they do not have or that a person has a sponsorship, approval, status, affiliation or connection that he does not have,"[61]

- "Representing that goods or services are of a particular standard, quality or grade, or that goods are of a particular style or model if they are of another,"[62]

- "Engaging in any other conduct which similarly creates a likelihood of confusion or of misunderstanding,"[63]

- "The act, use or employment by any person of any deception, fraud, false pretense, false promise or misrepresentation, or the concealment, suppression or omission of any material fact with intent that others rely upon such concealment, suppression or omission, in connection with the sale or advertisement of any goods or services, whether or not any person has in fact been misled, deceived or damaged thereby."[64]

In addition, the FTC's work in this area using a deceptive practices framework might help practitioners who are attempting to advance a data privacy cause of action. Finally, although the fines for UDAP violations are relatively minimal, the fee-shifting arrangement of the statute might make this a palatable avenue for attorneys to consider.

From a damages perspective, the general sentiment that many West Virginia consumers have expressed regarding the importance of their data should be used explicitly in one's valuation calculation. Typically, causes of action

---

60 One other potential challenge for the use of UDAP is the statute's requirement that the plaintiff incurred out of pocket expenses. *Id.* Presumably, however, the use of credit monitoring expenses that a plaintiff might have to use in cases associated with potential identity theft issues would be enough to satisfy the claim.

61 W. VA. CODE ANN. § 46A-6-102(7)(E) (West 2021).

62 *Id.* § 46A-6-102(7)(G).

63 *Id.* § 46A-6-102(7)(L).

64 *Id.* § 46A-6-102(7)(M).

based on rather amorphous concepts such as "privacy violations" are harder to evaluate. At a minimum, the fact that the general sentiment of prospective jurors is that the value of their data is significant should be a key factor in any evaluation of a case's worth. As West Virginia case law demonstrates, the fact that there may be no economic damage to a putative plaintiff does not automatically eviscerate the claim for significant damages.[65] Likewise, (as mentioned before) our findings from the initial survey showed the low level of trust that many respondents had regarding certain types of businesses (such as with e-mail providers and cell phone carriers). Practitioners may wish to consider this when developing cases that have these businesses as parties to the case.

V. CONCLUSION

Data privacy issues are intricate, interconnected, and important to understand. Given the predominance of technology in all aspects of our lives, tackling the regulatory framework might be the single greatest undertaking of this era. Moreover, the rapidity with which technology is changing makes the issue even more pressing—consider the fact that most individuals between the ages of 40 and 50 have seen the development, dominance, and now disuse of many technologies: video-cassette tapes, facsimile machines, and computer floppy disks. There is no reason to assume that this trend will not continue; in fact, it will likely accelerate. As such, developing foundational principles now—before our technology eclipses our moral regulation of it—will be a crucial legacy for us to leave to future generations.

---

65 Whitehair v. Highland Memory Gardens, Inc., 327 S.E.2d 438, 463 (W. Va. 1985).