Why was the FCC's Privacy Order Dead on Arrival? A New Approach to Evaluating Privacy Regulation

Victor Glass
Rutgers University

Abstract

The Federal Communications Commission issued a Privacy Order restricting the use of personal data by Internet Service Providers. Many consumer advocates hailed it as a bold step to protect personal privacy. Many Internet-based companies strongly disagreed. Shortly after the Trump Administration took office, the Privacy Order was repealed. This paper explains the controversies that led to the ultimate demise of the Order, assesses the debate using tools drawn from economic theory of the laws, introduces a new metaphor for privacy that could point to effective privacy rules, and finally uses the metaphor to suggest new directions for exploring privacy regulation.

Introduction

Broadband Internet Access Service (BIAS), which most people simply think of as Internet service, became a telecommunications service as a result of a Federal Communications Commission (FCC) Order released on March 12, 2015. Once BIAS became a telecommunications service, regulatory jurisdiction shifted from the Federal Trade Commission (FTC) to the FCC. (Some frequently used communication terms are explained in Table 1.)

As a newly classified telecommunications service, BIAS was potentially subject to all the rules associated with traditional plain old telephone service (POTS). Instead, the FCC decided on a "light touch" approach that exempted BIAS from many traditional regulations, but not from those related to protecting customer privacy. The exact privacy rules were going to be specified at a later date. On November 2, 2016, the FCC released its Privacy Order.[1] The order required an Internet Service Provider (ISP) inform customers of the intended use of their personal data; give customers veto

power over sharing personal information with other enterprises; assure the Commission that their databases are secure; and in the event of a data breach depending on its size, notify customers and government agencies in a timely manner.

Table 1. Communication Terms

Definitions
POTS: Plain Old Telephone Service, also known as a landline phone that carries voice traffic
BIAS: Broadband Internet Access Service, known simply as Internet service at speeds at least five times faster than voice service.
ISP: Internet Service Provider, a company that provides access to the Internet. Example: Verizon
Edge Provider: a company that provides content, applications, or services over the Internet. Example: Amazon

While these basic objectives sound reasonable, ISPs and companies that depend on ISPs to market their own services criticized the Order as unfair. The Association of National Advertisers (ANA) said the new rules would hurt their members' ability to target their marketing.[2] Oracle, a provider of cloud-based services,[3] said the rules would give Google an unfair advantage in the competition for advertising dollars.[4] Even Google opposed the rule that customers must opt-in to allow an ISP to view all of their web-browsing history. Google said, opt-in makes sense to protect sensitive health care information. It doesn't make sense for weather information viewed by a customer.[5]

On January 20, Politico Pro announced that the Trump administration selected Ajit Pai as the new chairman of the FCC.[6] Smart money was already betting as early as November 16, two-weeks after the Order's release, that it would either not be enforced or be withdrawn; there was even the possibility that BIAS would be reclassified as an information service, not subject to FCC control.[7]

True to expectations, on March 1, 2017, the Commission stayed part of the Order with more pushbacks to come.[8] On March 23, the Senate voted to kill the Privacy Order. Then on March 28, the House officially pronounced it dead by rescinding the Order.[9] President Trump signed its death certificate on April 3.[10] The Order's death leaves a regulatory vacuum because BIAS is still a telecommunications service—meaning the FCC, not the FTC, has

regulatory authority over it but has lost its ability to regulate ISP privacy practices. One way out is for Congress to kill the Net Neutrality Order that classified BIAS as a telecommunications service, and return control to the FTC.[11] Stay tuned, net neutrality may again become the next front-page battle with privacy protection as the rallying cause.

To understand the debate, this article: (a) summarizes the Privacy Order; (b) discusses the controversies that led to the Stay and ultimate demise of the Order; (c) assesses the debate using tools drawn from economic theory of the laws; (d) introduces a new metaphor for privacy that could point to effective privacy rules; (e) uses the metaphor to suggest new directions for exploring privacy regulation.

Privacy Order: Introduction and Summary

One saving grace for Internet customers has been that many of the big ISPs are the old telephone companies. They have a history of protecting individual privacy—but, even that sense of security must be eroding with revelations of massive data leaks by other large on-line businesses. Besides, the old telephone companies no longer act like Ma Bell. They are trying to compete with Comcast, YouTube, Amazon, and many other on-line platforms. They routinely build profiles of personal likes and dislikes and use them to customize their data plans. Verizon recently bought Yahoo to expand its digital media business.[12] With so many huge on-line companies gathering personal data, the Internet, in Daniel Solove's words, is quickly becoming Kafkaesque.[13] Large, faceless bureaucracies are spying on the public, and we, the public, are becoming anxious that there is no way to get control of our personal identities.

One of the biggest type of online bureaucracy is the ISP. For example, Verizon had 160,000 employees in 2016.[14] It is not hard to imagine a consumer believing that BIAS is a take-it-or-leave it proposition. If you want Internet service from a particular ISP, you must take the advertised price and allow the ISP to use your personal information as it sees fit.

The FCC's Order attempts to empower consumers who feel helpless. The Order articulates three foundations for its ISP privacy regulations aimed at giving customers control over their personal data: transparency, choice, and security.[15]

Transparency

Informed customers must have the right to

1. Know the specific information that is being collected about them
2. Be given proper notice that such information is being used for other purposes

3. Be allowed to stop the reuse or sale of that information.[16]

Choice

The type of consent required that allows an ISP to use specific information depends on whether the FCC judges personal data to be sensitive or not. The Order defines three types of proprietary information protected under Section 222 as sensitive:

1. Individually identifiable Customer Proprietary Network Information (CPNI) as defined in Section 222(h).
   CPNI includes billing information and network routing information that could identify a customer.[17] Examples of CPNI are the type of broadband service bought, customer premises equipment information, Internet Protocol (IP) addresses, traffic statistics information, and application information.[18] Application information can include websites visited or emails sent or received.[19] CPNI also includes geo-location information.[20] To harmonize old POTS privacy regulations with BIAS regulations, the Order classifies both IP addresses and telephone numbers as CPNI.[21]
2. Personally identifiable information (PII).
   PII includes any information reasonably linked or linkable to a device.[22] Examples are Social Security Number, date of birth, mother's maiden name, and government identifiers such as a driver's license, physical address, email address, phone numbers, and other unique identifiers. Some PII categories are also CPNI categories.[23]
3. Content of communications.[24]
   Content of communications includes "any part of the substance, purport, or meaning of a communication or any other part of a communication that is highly suggestive of the substance, purpose, or meaning of a communication." Examples of content includes, but is not limited to, the "contents of emails; communications on social media; search terms; web site comments; items in shopping carts; inputs on web-based forms; and consumers' documents, photos, videos, books read, [and] movies." The list is not exhaustive.[25]

The Order gives customers two types of choices: opt-in and opt-out.

1. Opt-in applies to use of personal, network, and content information that can be used to profile an individual. Material changes in an ISP's privacy policy also requires opt-in from the customer.[26]
2. Opt-out is a choice for non-sensitive personal information such as data related to the Internet of Things (IoT) such as home security and home automation.[27] Opt-out is required for direct marketing (first party marketing) to the customer.[28]

An ISP does not need customer consent to use personal data to

1. Initiate, render, bill, and collect for telecommunications services
2. Protect the rights or property of the carrier, or to protect users and other carriers from fraudulent, abusive, or unlawful use of, or subscription to telecommunications services
3. Provide any inbound telemarketing, referral, or administrative services to the customer for the duration of a call
4. Provide customer location information and non-sensitive customer PI in certain specified emergency situations.[29]

No consent is necessary for de-Identified Information because it is not personally sensitive. De-identified data must pass a three-part test articulated by the Federal Trade Commission (FTC):

1. The information is not reasonably linkable to an individual or device
2. The ISP publicly commits to maintain and use the data in a non-individually identifiable fashion and to not attempt to re-identify the data
3. The ISP contractually prohibits any entity to which it discloses or permits access to the de-identified data from attempting to re-identify the data."[30]

Security

Besides empowering the customer, the Order helps assure the public that ISPs will protect their privacy – at least to some extent – once they have gathered sensitive data. The Order defines data security and breach notification requirements that stress the fiduciary responsibility of an ISP to protect sensitive information entrusted to them.

According to the Order, data security refers to unauthorized access and disclosure—in other words, it refers to hacking.[31] The Commission expects ISPs to adhere to a "reasonable measures" standard for Data Security and Breach Notification and recommends that ISPs adopt best industry practices techniques.[32] For example, the data security framework should be consistent with the Cybersecurity Framework (NIST CSF) used by edge providers, that is by companies that offer content, applications, or services over the Internet.[33] The Commission recognizes, however, that other frameworks are also being used.[34]

Best practices typically include a written data security program, designation of senior managers personally responsible for data security, and training employees and contractors on the proper handling of customer data. String authorization procedures are useful, and so is "data minimization" and safe disposal of data.[35]

The Order specifies that the "reasonable" standard is different for large compared to small ISPs because security measures that may be appropriate for larger providers, such as having a dedicated official to oversee data security implementation, are likely beyond the needs and resources of the smallest providers.[36]

Data Breaches and Notifications

When databases are breached, the Order requires ISPs to inform customers and law enforcement agencies as soon as reasonably possible. Depending on the severity of a data breach, an ISP must notify affected customers, the Commission, the FBI, and the Secret Service. The Order defines "harm" as a concept that can be broadly construed to encompass "financial, physical, and emotional harm" The FCC finds that "within the meaning of Section 222(a), threats to the "confidentiality" of customer personal information include not only identity theft or financial loss but also reputational damage, personal embarrassment, or loss of control over the exposure of intimate personal details."[37]

Notification applies to encrypted data because of the likelihood that it can be decrypted.[38] Notification is also required when a provider is unable to determine the scope of the breach.[39]

Government notification

Government notification depends on the number of people affected and the potential harm that may have occurred. Breaches affecting 5,000 or more customers require carriers to notify the Commission, the FBI, and the Secret Service within seven (7) business days of when the carrier reasonably determines that a breach has occurred, and at least three (3) business days before notifying customers. For breaches affecting fewer than 5,000 customers, carriers must notify the Commission without unreasonable delay and no later than thirty (30) calendar days following the carrier's reasonable determination that a reach has occurred. Both of these thresholds remain subject to the harm-based trigger.[40]

Customer Notification

Customer notification of a breach lags behind government notification. The FCC requires BIAS providers and other telecommunications carriers to notify affected customers of reportable breaches of their customer PI without unreasonable delay, and no later than 30 calendar days following the carriers' reasonable determination that a breach has occurred, unless the FBI or Secret Service requests a further delay.[41]

Information provided to a customer after a breach must, at a minimum, include: the date; the personal information breached; a contact number for the telecommunications carrier and FCC; and if the breach will cause financial harm, information about national credit-reporting agencies and steps customers can take to guard against identity theft.[42]

Trading Privacy Data

The Order allows customers to trade personal information for ISP price discounts on Internet service. Customers can't effectively make this trade if an ISP gives a customer a take-it-or-leave it ultimatum to surrender all privacy rights in exchange for Internet service. As a result, the Order prohibits ISPs such offers and uses Sections 222 and 201 of the Telecommunications Act to justify its prohibition.[43]

Allowing BIAS price discounts in exchange for personal data follows a commonplace practice in the digital marketplace. Examples include customer loyalty programs that track customer purchasing habits. Anyone who has a supermarket price discount card knows that he is trading lower prices for revealing personal buying habits. In general, The FCC believes financial incentives benefit both consumers and companies as long as the incentives are based on informed consent.[44]

One potential drawback of price discounts is that customers do not know the value of their personal information. It may cost customers $62/month to protect their privacy by not allowing the ISP to use their personal data for marketing purposes. This is an expensive sacrifice, especially for low-income customers. To make the trade more transparent, the provider must explain to the customer how the data will be used. The FCC will closely monitor these incentive programs to make sure that the discount plans are mutually beneficial to customers and ISPs.[45]

Exemptions

Large business customers, called enterprise customers, that purchase sophisticated private network services are exempt from these rules because they have bargaining power to protect their privacy and security needs. Enterprise contracts typically address issues related to transparency, choice, data security, and data breach, and define ways for an enterprise customer to communicate privacy concerns to the network provider. When these issues are not addressed in an enterprise contract, the privacy rules defined by the Order will apply. The exemption also does not apply to the purchase of BIAS services.[46]

Preemption of State Law

The Order preempts state privacy and breach laws only when they are inconsistent with the rules adopted in the Order.[47]

Summary of Controversies and the Stay

Despite widespread agreement that customers need privacy protection, ISPs and others said the Order is on the wrong track. Even within the Commission, the Order drew sharp criticism. As with previous orders under the Wheeler chairmanship, the commissioners allied with the Republican Party dissented but were in the 3-to-2 minority. Although the Order is now dead, the reasons given to support or object to the Order will carry over to future debates on Net Neutrality and Privacy.

The Commissioners in the majority, Wheeler, Clyburn and Rosenworcel, focused on empowering individuals so that they could control the personal information they share with ISPs. Wheeler said, "it's your data. How it's used and shared should be your choice."[48]

Clyburn verbalized the common feeling that customers don't feel they have a choice.

> Ninety-one percent of Americans believe they have lost control of their personal information. This is not surprising when the new normal includes cyberattacks, massive data breaches, and revelations about companies selling data to government agencies.[49]

Clyburn didn't believe the Order would empower consumers completely, but, at least, additional consent would give them more say about how their personal information is used.[50]

Rosenworcel expressed the public angst caused by widespread exchange of Internet data.

> Unlike in the past, when relationships were mainly between customer and carrier, in the digital age third party participation has expanded exponentially.
>
> Dial a call, write an e-mail, make a purchase, update a profile, peruse a news site, store photographs in the cloud, and you should assume that service providers, advertising networks, and companies specializing in analytics have access to your personal information.
>
> Lots of it. For a long time. Our digital footprints are no longer in sand; they are in wet cement.[51]

She said an uneasy public is grappling with the tradeoffs of a fundamentally new dimension to life. Although the Internet holds so much promise for bettering our lives, like any revolutionary change in technology it also can become a weapon for exploiting the public. For example, she said, the future of the world is the Internet of Things (IOT).

> [IOT] creates powerful opportunities that will make us more effective and more efficient, our cities smarter and our communities more connected. But these benefits come with big security challenges. We had an object lesson in these challenges … with one of the largest Distributed Denial of Service attacks in history, with botnets taking control of insecure connected devices, and compromising them by flooding servers and sites with overwhelming traffic.[52]

In this new landscape, Rosenworcel reflects that consumers wonder what privacy means. The public wants the right to be left alone. They want control of their personal information. She concludes by saying that the Commission has provided tools to do just that. The Order focuses on transparency, choice, and security. She believes another should be simplicity. Consumers should not have to be network engineers or lawyers to understand if their information is protected.[53]

The two dissenters on the Commission, Pai and O'Rielly, believe the Order doesn't really protect customers. Instead, it would likely lead to customer confusion, an undeserved sense of security, and handicap ISPs in the digital marketplace.

Pai began his broadside by attacking the Order for handicapping ISPs in the digital marketplace. He said regulation should be competitively neutral. Unfortunately, the Order doesn't meet this requirement because there are now two sets of regulations operating to control Internet behavior.

> The FTC has for the past two decades developed a technology-neutral framework for privacy that applied to all sectors of the on-line community. … It didn't matter if a company was an edge provider or an ISP.[54]

He goes on to say that imposing rules on ISPs that would not apply to edge providers is not optimal regulation. FCC regulations should be harmonized with those of other federal agencies, but they are not. Instead, ISPs now face a different set of rules than edge providers, which was not the case when Internet privacy regulations were developed by the FTC. Two sets

of rules make no sense to Pai. And there is no justification for treating ISPs differently than edge providers. Saying ISPs see vastly more data than edge providers doesn't make sense in the age of Big Data. Google, Yahoo, Twitter, and Facebook, and Microsoft Skype are routinely invading privacy. They have more insights into customer behavior than ISPs. Yet, this Order subjects ISPs to more stringent regulations than apply to edge providers. Consumers want consistent Internet privacy rules. Pai suggests that the FTC will have to amend its privacy regulations to conform to the FCC's.[55]

Michael O'Rielly, the other dissenter, believes the Order was more a product of political infighting than cool rational economic analysis. He believes the FCC's foray into privacy regulation is nothing more than a power grab disguised as a public service. He said "The FTC's system was working quite well. Not content, "the FCC [has] embarked on an expansionist policy," without any legal basis. In his words, the FCC has twisted the meaning of Section 222 of the Act, which applied to privacy regulations for voice service, and applied it to BIAS. Besides the proprietary data the FCC is so concerned about is widely available from data brokers.[56]

Opt-in for web browsing makes no sense according to O'Rielly. He said the FTC doesn't treat web-browsing data as sensitive, and "There is no evidence of privacy harms, and businesses have been able to provide discounts, convenient features, and other innovative services." It will also create confusion, according to O'Rielly. A customer may not opt-in to the ISP but see advertisements on an ISP website generated by edge providers who have this information based on an opt-out decision.[57]

He noted that the public doesn't really choose. A rule of thumb is that 82% of customers default with an opt-out option and 18% actually choose to make a decision. If the ratios are similar, opt-in will cause a significant loss of marketing data for an ISP. ISPs will have to purchase this information. They may do so by offering price incentives to their customers to opt-in, but any price concession offered will be reviewed on a case-by-case basis by the FCC – an agency that has no experience judging them. An alternative is to purchase data from data brokers or edge providers. In effect, the opt-in rule raises ISP costs and tilts ground rules in favor of edge providers. The uneven playing field will likely lead to less investment in new services by network providers.[58]

O'Rielly warned edge providers that opt-in is not a clear win for them. Most troubling of all to O'Rielly was that the FCC, under Wheeler, was thinking of extending its privacy rules to the Internet of Things (IoT). The edge community needs to watch out. The FCC may be overseeing their privacy practices, which, till now, was in the FTC's sole jurisdiction and subject to opt-out regulation.[59]

After the Order was released and the dissent documented, the FCC, under the newly appointed chairman, Commission Pai, the FCC stayed part of the Order related to data security and stated the other privacy regulations would not be stayed "at this time."[60] The justification for staying the data security rules is that there is no mechanism to assure that the FCC's definition of its "reasonableness" standard will be consistent with the FTC's definition, which applies to other companies in the Internet market.[61]

Assessing the Debate Using Privacy Standards based on Enhancing Wealth

The Privacy Order's prime objective is to protect the public's privacy in the digital age. The articulated rules are based on a data sensitivity standard. An ISP that wants to use sensitive data for other than the service purchased must clearly inform customers of its intentions, must allow customers to choose whether to consent to the intended use, and must protect the sensitive data it has.

An alternative to the sensitivity standard is a wealth enhancing standard. It offers a second look at the effectiveness of the Order's privacy regulations. This alternative approach is firmly grounded in the "economics of the law" literature.[62] It is the standard most consistent with explaining Pai and O'Rielly's attacks on the Order.

The basic assumption of the economic approach to privacy is that effective laws are wealth enhancing. In general, laws should be enacted when the expected reduction in losses is larger than the burden of compliance.[63] Moreover the liability should fall on the party most responsible for an accident or personal injury.

As Richard Posner pointed out, the wealth enhancing standard for the law is not ethically neutral. People have basic rights that must be protected and beyond that the law should maximize utility.[64]

Economic Causes of Privacy Protection Failures

The standard economics of the law analysis begins with identifying market failures associated with high external costs, high transaction costs and pockets of market power.

Market Failures

1. High External Costs. Privacy is not a well-defined concept, let alone a simple commodity that can be bought and sold. The standard legal definition is actually based on four types of unwanted exposure or theft of personal information: (1) intrusion upon seclusion; (2) public disclosure of private facts that are offensive and not a legitimate

concern of the public; (3) characterizing in a false light; and (4) appropriation of one's identity.[65] Each category rests on a specific type of invasion of privacy. The categories do not include digital mosaics built from seemingly harmless data that can be viewed on-line. Digital Mosaics raise a basic question that has been outstanding since at least the invention of the camera. No one presumes all pictures are private. A person's picture in a crowd is not a personal asset that can be sold. Even when personal data is judged to be private, it is not like standard commodities. In a traditional commodities market, a trade transfers ownership from seller to the buyer. This is not true of personal data. Ownership is never completely transferred. A customer retains rights to the data revealed to an ISP. When an ISP or any other Internet-based company uses in unexpected ways, it could lead to large personal losses: identity theft, pictures that cause shame, opinions half-thought-out that distort a person's character, and reveal membership in a protected group that could lead to unwarranted personal discrimination. The costs of even small privacy invasions can produce changes in society that are socially harmful. Fear of potential privacy invasion, even when actually small, can chill candidness and individuality. People will present a false image to the world to protect themselves. Conformity and political correctness serve as an insurance policy against future attacks. Citizenship can be stunted when one is afraid of building a record of inconsistencies and backtracking that can be used as a weapon against anyone running for public office.[66] Lifting trade secrets or the fear of being hacked can freeze innovativeness if all one's work can be pieced together from the Internet, or hacked from one's personal computer and databases.

2. High Transaction Costs. A typical person's digitized information floats through the web. It is difficult to identify its users, difficult to tell how it is being used, and difficult to identify its value. Users of digitized data may need different bundles of personal characteristics for their marketing efforts. The valuation problem gets more complicated because personal information becomes valuable when bundled with the information of others. Typically, service providers use aggregate behavior patterns to make market recommendations or develop new services. Big Data tools are not reliable for predicting individual customer behavior. Often data are treated like prospecting fields. Companies try to identify behavioral patterns that are not well understood or even defined. As a result, a privacy statement that explains the use of the data will likely be vague. All of these

considerations suggest the market for specific data will be hard to set and contracting will be very costly with individuals.

3. Pockets of Market Power. Large ISPs, edge providers, and data brokers may have the power to behave opportunistically. The FCC presupposes the ISPs have classic market power by having access to personal information that edge providers cannot acquire easily. It is also likely that large Internet players, ISPs and others, have more bargaining power than individual customers, and therefore, can force customers to reveal personal data.

Regulatory Agency Failures

Market failures don't automatically justify regulatory intervention. Regulations are also costly for a variety of reasons:

1. Regulations Standardize Practices. Internet privacy standards may not be efficient in the near- and long-term. Fiber optics, packet switching, the growth of virtual private networks, the development of Big Data, and new products and services offered on-line suggest that static rules become obsolete very rapidly in the digital world. If privacy becomes an important marketing tool, companies will have an incentive to secure their website and plainly tell customers that they will hold to explicit privacy standards. They will invest in secure databases and publicize their track records for data security. Having a regulator set privacy standards may stifle innovative competitive responses to privacy fears and invasions.
2. Regulatory agencies Multiple Objectives. Protecting personal privacy is one of several regulatory agency objectives. In the FCC's case, for example, it has tried to jump start competition for network services and promote universal service. The end result is that market efficiency may be sacrificed for other social objectives.
3. Regulatory Agencies have Jurisdictional Limitations. Many government agencies offer the public privacy protection for certain types of services. This silo effect can lead to inconsistent rules and competitive disadvantages in the marketplace.
4. Regulatory Agencies Compete. Jurisdictional lines do not have bright lines. As a result, agencies may compete to expand their regulatory authority. This may be done by introducing rules that overlap with another agencies.

Using the wealth enfacing framework, assuming market and regulatory failures are true, they can be used to explain why Pai and O'Rielly protested against the Privacy Order. Consider again, transparency, opt-in, opt-out, and

data security issues from this perspective. The focus shifts from data sensitivity to efficient markets.

Transparency

Pai and O'Rielly did not attack the transparency objective because lack of disclosure or buried disclosures are a fact of life in BIAS agreements. The real issue is whether the Order's disclosure requirements would really better inform the public. Perhaps. But even now customers hardly look at customer agreements. Is it because no matter how simple or explicit the terms of the agreement, they do not really understand the terms and conditions? Are they fatigued by reading multiple consent forms? Are they more likely to watch YouTube style instructions than written ones? The FTC is on record as supporting transparency.[67] The dissenters simply believe the FTC should take the lead in answering these questions.

Opt-in

Opt-in, in theory, mimics standard buyer behavior in traditional markets where a consumer must agree to buy the product at the advertised price. In practice, opt-in doesn't translate well in the digital world because customers don't know what they are really opting into and don't seem to feel that they have control over what they consider to be personal and private. Low opt-in rates may force an ISP to buy data, perhaps from customers. This could be through promotions or selected price discounts. Or the ISP could buy the information from a data broker. If the company is in a competitive market, the predicted results would be that the average price to all customers will go up to pay for the price discounts to targeted customers or for the cost of purchasing data from a broker. To the extent that less net information is collected from customers, opt in may lower data leaks – unless data brokers or edge providers already have it. This narrative explains why Pai and O'Rielly believe the opt-in choice may have limited success reducing unwanted data releases at the expense of giving data brokers and edge providers an unfair competitive advantage.

Opt-out

Opt-out keeps ISPs on the same regulatory footing as their competitors. It allows ISPs a level playing field to develop home security and home automation Internet of Things (IoT). The puzzling explanation that IoT does not yield personally sensitive data is hard to understand. The privacy risks associated with monitoring a smart home, for example, are enormous. The viewer can learn a household's personal habits; when they are at home; when they are on vacation. The point is that the Order's artificial segmentation of

sensitive and non-sensitive data shows that the sensitivity standard is faulty. Besides that, it will need constant updating as smart appliances and machine-to-machine communications add new streams of personal data to the Internet flow. Again, by the FCC's own admission, few customers exercise their opt out right. As a result, opt out is not likely to offer much privacy protection.

The FTC was already regulating Internet services through its customer protection mandate. Now two agencies are covering similar territory. This is likely to cause customer confusion and regulatory in-fighting.

Data Security

Pai and O'Rielly believe the FTC is doing a credible job and has experience at evaluating data security and breach. The Order, itself, relies on best practices defined by the FTC.[68] Again, why have the FCC coopt the FTC? From their perspective, the FCC is trying to poach in the FTC's domain. They are also worried that the FCC will not use the same test and have the same scoring measure as does the FTC, which will cause costly database redesigns that are unnecessary.

Recommendations Using the Wealth Maximization Standards

The FCC spent millions of dollars to investigate market power in the Business Data Services market, which it sized at $45 billion. It seems odd not to conduct a market assessment of ISP market conduct and performance in the Internet. Verizon's purchase of Yahoo suggests that ISPs lack market power because of limited product offerings.

A unifying metaphor helps focus research on market failures. Solove suggested that the digital age has created a Kafkaesque environment. The public knows that huge bureaucracies have collected personal data but have no idea how it is processed, and have no idea whether they are being profiled or secretly judged. His metaphor highlights the loss of control in a society run by bureaucracies. It also explains the positions of Wheeler, Clyburn, and Rosenworcel. They want to open the doors to bureaucracies to let the public see what bureaucrats are doing with their data.

An alternative metaphor that may appeal to Pai and O'Rielly is based on digital mosaics. A Digital Mosaic (DM) is a profile pieced together from data available through the Internet. A DM can portray a person, a company, an activity, or any other potentially valuable Internet byproduct. DM's stimulate the development of new products to meet customer needs that have not been served.

In the process of using and trading data, personal memes for developing customer profiles, shards of personal data float throughout the Internet can

also create digital mosaic pollution (DMP). It is the equivalent of bits of dirt that can be collected and piled in dump sites used by unscrupulous individuals, businesses, and governments to invade a person's privacy for bad reasons: to peek, to humiliate, to control, and to steal. Other shards can be gathered to spy on businesses.

In the wrong hands, DMP can cause personal and social damage by polluting the Internet landscape with false or deceptive images. Once out there, these digital shards of information are very difficult to clean up, and can be used in ways that can invade privacy. The DMP metaphor suggests a shortcoming of privacy law is that it doesn't address seemingly harmless leakages of private data that pose a large societal threat, a problem raised by Solove and others. Opening doors to large bureaucracies and giving the public a say in their operations are not enough to prevent seemingly harmless DMP.

DMP invokes a variety of pollution images that could focus research and suggest when government intervention would be most effective. It is not hard to imagine DMP spewing from private Internet companies and public institutions that gather a great deal of personal information. It is not hard to imagine pools of data that are toxic or can become toxic. It is not hard to imagine taxes to limit DMP or institutional regulations to limit uncontrolled spewing of data at its source. It is not hard to picture removing digital pollution that already exists. It is not hard to picture maps that trace the source of DMP and its destinations, or time elapsed maps that show how DMP is evolving. Perhaps these types of maps could answer to what extent on-line markets heal themselves. Many legal scholars assume markets can solve the DMP problem.[69] Many do not.

A reasonable assumption is that DMP is not possible to eliminate, but laws can help limit DMP to economically efficient levels. A great challenge is to quantify the costs of DMP. For some types, it may be impossible. Whatever measures are developed, laws based on them should be technically and competitively neutral and should apply to the three main sources of Internet data: Internet Service Providers (ISPs), edge providers such as Amazon, Facebook, and Google, data brokers such as Wiland Services, and government agencies.[70]

The next issue is what types of laws will be most effective. In a fast-changing environment, preemptive rules are not likely to work effectively and may stifle innovation. The case-by-case method adopted by the FTC may be best because it doesn't presume the government knows better than the private sector how to correct failures. Rulings recognize the clash of legitimate interests and weigh them based on historical precedent and the facts of the case. It is admittedly a process that crawls into the future. But

consider this: a policy maker who wants sweeping legislation should reflect on changes in on-line data security that have evolved. Companies like Apple offer encrypted messaging. ISPs offer virtual private networks to deliver sensitive data. The private sector fixes problems that the public is willing to pay for.

Privacy rules should shift from "let the buyer beware" to "let the seller beware." ISPs and edge providers like Google should know the risks associated with handling and trading sensitive information. They know the likelihood of re-identifying seemingly de-identified data. They know that consumers are unlikely to check their use of sensitive data. They know if they are stealing business secrets from their competitors.

One government agency should develop privacy regulations. By default, the FTC has regulated Internet privacy. It should continue to do so and have its regulatory powers extended to communication network providers. The FTC should work collaboratively with the FCC, which has had responsibility for carrier privacy rules. Perhaps a new agency should be formed to oversee network security that could include not only the Internet but other networks that are becoming intelligent. A case in point are the smart networks being developed by the electric utility industry.

In the meantime, it will be up to private organizations to develop privacy standards. The death of the Privacy Order has left an oversight vacuum that needs to be filled.

Author

Dr. Glass is Director, CRRI Scholar, and Professor of Professional Practice - Finance and Economics, Rutgers Business School - Newark and New Brunswick, Rutgers University. Prior to joining Rutgers, Dr. Glass was Director of Demand Forecasting and Rate Development at the National Exchange Carrier Association. For almost thirty years, he was responsible for forecasting demand and setting switched and special rates for more than 1100 telephone companies. He was heavily involved in access restructure, universal service reform, and new access services. He is the lead author of many business and academic studies. Dr. Glass earned his MBA in marketing and finance, and Ph.D. in economics from Columbia University.
email: vglass@business.rutgers.edu

Endnotes

1. Federal Communications Commission. (2016). *Protecting the privacy of customers of broadband and other telecommunications services* (FCC Report and Order, 16-148). Federal Communications Commission. Retrieved from https://apps.fcc.gov/edocs_public/attachmatch/FCC-16-148A1.pdf
2. David, W. (2017, January 24). ANA expects Trump FCC pick to revisit privacy. *MediaPost*.

Retrieved from http://www.mediapost.com/publications/article/293642/ad-industry-expects-new-fcc-chair-to-revisit-priva.html
3. Oracle Corporation. (n.d.) In Wikipedia. Retrieved from https://en.wikipedia.org/wiki/Oracle_Corporation
4. Davis, W. (2016, December 21). Oracle petitions FCC to reconsider broadband privacy rules. *MediaPost*. Retrieved from http://www.mediapost.com/publications/article/291639/oracle-petitions-fcc-to-reconsider-broadband-priva.html
5. Bode, K. (2016, October 6). Google argues against tougher broadband privacy rules. DSL Reports. Retrieved from http://www.dslreports.com/shownews/Google-Argues-Against-Tougher-Broadband-Privacy-Rules-138049
6. Heitmann, J.J., Dempsey, J., & Slutsky, R. (2017, January 22). Ajit Pai selected as next FCC chairman. *CommLaw Monitor*. Retrieved from http://www.commlawmonitor.com/2017/01/articles/business-strategic-planning/ajit-pai-selected-as-next-fcc-chairman/
7. Coie, P. (2016, November 15). FCC's Broadband Privacy Order: Dead on Arrival? *JDSupura*. Retrieved from http://www.jdsupra.com/legalnews/fcc-s-broadband-privacy-order-dead-on-12827/
8. Federal Communications Commission. (2017). *Protecting the privacy of customers of broadband and other telecommunications services* (FCC Report and Order, 17-19). Federal Communications Commission. Retrieved from https://transition.fcc.gov/Daily_Releases/Daily_Business/2017/db0301/FCC-17-19A1.pdf
9. Fenlon, W. (2017, March 28). Goodbye internet privacy: U.S. House of Representatives just killed FCC privacy rules. *PC Gamer*. Retrieved from http://www.pcgamer.com/goodbye-internet-privacy-us-house-of-representatives-just-killed-fcc-privacy-rules/
10. Brodkin, J. (2017, April 3). President Trump delivers final blow to Web browsing privacy rules. *Ars Technica*. Retrieved from https://arstechnica.com/tech-policy/2017/04/trumps-signature-makes-it-official-isp-privacy-rules-are-dead/
11. Kang, C. (2017, March 23). Congress moves to strike Internet privacy rules from Obama era. *New York Times*. Retrieved from https://www.nytimes.com/2017/03/23/technology/congress-moves-to-strike-internet-privacy-rules-from-obama-era.html
12. Ha, A. (2017, February 15). Verizon reportedly closes in on a Yahoo acquisition with a $250M discount. *TechCrunch*. Retrieved from https://techcrunch.com/2017/02/15/verizon-yahoo-250-million/
13. Solove, D. (2004). *The Digital Person*. NY: New York University Press.
14. Number of employees at Verizon from 2007 to 2016. (2017). *Statista*. Retrieved from https://www.statista.com/statistics/257304/number-of-employees-at-verizon/
15. Federal Communications Commission. (2016). *Protecting the privacy of customers of broadband and other telecommunications services* (FCC Report and Order, 16-148, par. 7). Federal Communications Commission. Retrieved from https://apps.fcc.gov/edocs_public/attachmatch/FCC-16-148A1.pdf
16. Ibid., par. 21
17. Ibid., par. 47
18. Ibid., par. 53
19. Ibid., par. 58
20. Ibid., par. 65
21. Ibid., par. 68
22. Ibid., par. 89

23. Ibid., par. 93
24. Ibid., par. 6
25. Ibid., par. 103
26. Ibid., par. 195
27. Ibid., par. 198
28. Ibid., par. 199
29. Ibid., par. 201
30. Ibid., par. 106
31. Ibid., par. 239
32. Ibid., par. 245
33. Ibid., par. 246
34. Ibid., par. 250
35. Ibid. par. 251-254
36. Ibid., par. 243
37. Ibid., par. 261, 263, 266
38. Ibid., par. 269
39. Ibid., par. 273
40. Ibid., par. 278
41. Ibid., par. 284
42. Ibid., par. 288
43. Ibid., par. 12 and 295
44. Ibid., par. 298
45. Ibid., par. 303
46. Ibid., par. 15, 306, 307, 308
47. Ibid., par. 20
48. Ibid., pp. 204
49. Ibid., pp. 205
50. Ibid., pp. 205
51. Ibid., pp. 207
52. Ibid., pp. 207
53. Ibid., pp. 207, 208
54. Ibid., pp. 209
55. Ibid., pp. 209, 210, 211
56. Ibid., pp. 212, 213
57. Ibid., pp. 215
58. Ibid., pp. 216, 217, 218
59. Ibid. pp 216
60. Federal Communications Commission. (2017). *Protecting the privacy of customers of broadband and other telecommunications services* (FCC Order Granting Stay Petition in Part, 17-19, par. 1). Federal Communications Commission. Retrieved from https://transition.fcc.gov/Daily_Releases/Daily_Business/2017/db0301/FCC-17-19A1.pdf,
61. Ibid., par. 4-5
62. This modern method originated with Coase and Calabresi, and was extended by Posner and others to examine privacy laws. See Veljanovski, C. (2007). *Economic Principles of Law*. Cambridge, UK: Cambridge University Press.

63. See Learned Hand Test in Veljanovski, C. (2007). *Economic Principles of Law* (pp. 186-190). Cambridge, UK: Cambridge University Press.
64. Posner, R. (1981). *The Economics of Justice*. Cambridge, MA: Harvard University Press.
65. Solove, D. (2004). *The Digital Person*. NY: New York University Press.
66. See Cohen, J. E. (2013, May 20). What is Privacy For? *Harvard Law Review*. Retrieved from http://harvardlawreview.org/2013/05/what-privacy-is-for/
67. Federal Communications Commission. (2016). *Protecting the privacy of customers of broadband and other telecommunications services* (FCC Report and Order, 16-148, par. 126). Federal Communications Commission. Retrieved from https://apps.fcc.gov/edocs_public/attachmatch/FCC-16-148A1.pdf
68. Ibid., par. 240
69. See William Prosser's categorization in Solove, D. (2004). *The Digital Person* (pp. 58). NY: New York University Press.
70. Solove, D. (2004). *The Digital Person*. NY: New York University Press.