"IP"SO FACTO? NOT SO FASTO: WHY IP ADDRESSES SHOULD NOT BE CONSIDERED PII

TIM LACHANCE*

ABSTRACT

Privacy law is an expansive and growing practice area, and there is much debate about how far the right to privacy extends, including to what extent consumer privacy must be protected. With the advent of the internet age, and the subsequent explosion of consumer technology, the question of what personal information should be kept private, and how such privacy should be achieved has likewise become more and more complicated. Among these complications is the question of whether Internet Protocol (IP) addresses – the facilitators of all internet communications – should be considered Personally Identifiable Information (PII). Because IP addresses are inherently different from traditional PII in terms of (1) their dynamicity, (2) their definiteness, and (3) the potential risk of harm their disclosure poses, IP addresses should not be deemed PII. However, the law is a creature of compromise, and there may be room for a solution that protects IP addresses at the point where they are most vulnerable, while mitigating the potential liability of actors lacking the necessary knowledge or resources to properly protect them.

* J.D. Candidate, 2018, University of New Hampshire School of Law.

I. INTRODUCTION

Governments around the world have long protected the privacy of what is known as "personally identifiable information" (PII). That is, information deemed to be of such a nature that an individual's identity could be determined with its use. With the advent of the internet age, there has been much discussion about whether Internet Protocol (IP) addresses should be considered PII, subject to the same protections as "traditional" PII, such as phone numbers, e-mail addresses, and names. Arguments have been made on both sides, and there is no clear, definitive

answer to the question, although trends have developed in certain jurisdictions.

This note makes the argument that, although some jurisdictions have chosen to classify IP addresses as PII (mainly European), U.S. law should reject this notion, as IP addresses can only ever identify machines, and not persons. Further, this is an age in which businesses are essentially required to have an internet presence, or risk missing out on a large customer base. This is true from the biggest of box stores, to the smallest of local businesses and startups. Requiring these businesses to implement an IP address management and protection plan, while opening them up to potential civil liability if such a plan fails, adds unnecessary and unsupportable regulatory costs, not justified by the potential risk to website visitors.

Part I of this note provides an overview of IP addresses, how they work, and what they indicate. Part II details where the law currently stands on PII, its definition, and how it has been applied to IP addresses. Part III lays out the argument that IP addresses should not be considered PII, because they are inherently different from traditional forms of PII, and defining them as such would impose unreasonable costs on businesses saddled with their protection. Finally, Part IV details a potential solution (which may already have been effectively implemented) for protecting IP addresses at the service provider level, where IP addresses have their only real potential of being connected to any individual.

II. HOW IP ADDRESSES WORK

IP addresses are unique strings of numbers assigned to a computer (or other internet connected device) which serve to identify the machine and facilitate online

communications.[1] The term "address" is an apt description. IP addresses act like house numbers, they tell the delivery service where a message is going to, and coming from, just like the addresses on an envelope.[2] If there are no IP addresses, the delivery system does not know where to send a communication. Every communication across the internet includes the IP addresses of both the sending and receiving parties.[3]

There are two major IP address systems currently in use: IPv4 and IPv6.[4] IPv6 was developed as a replacement for IPv4, providing an exponentially greater number of addresses than is available with IPv4, the addresses of which are being exhausted by the increasing number of internet connected devices.[5] However, IPv6 is still not widely used at this time, and will not be discussed here.

IPv4 addresses consist of a string of four number sets called "octets," each separated by a dot.[6] For example: 192.16.254.1

This string of numbers indicates both the individual machine being used, and the network on which that machine is residing.[7] The first one to three octets identify the network, and the remaining sets the individual machine.[8]

IP addresses can be either "static" or "dynamic."[9] A static IP address is permanently assigned to an individual

---

[1] Joshua J. McIntyre, *Balancing Expectations of Online Privacy: Why Internet Protocol (IP) Addresses Should Be Protected as Personally Identifiable Information*, 60 DePaul L. Rev. 895, 899-900 (2011).
[2] *Id.* at 900.
[3] *Id.*
[4] CHARLES R. SEVERANCE, INTRODUCTION TO NETWORKING: HOW THE INTERNET WORKS 37-8 (1st ed. 2015).
[5] *Id.* at 48-9.
[6] *Id.* at 37.
[7] SEVERANCE, *supra* note 4, at 38.
[8] *Id.*
[9] McIntyre, *supra* note 1 at 900.

computer, and never changes.[10] However, because IPv4 contains a finite set of possible addresses (around four billion), not enough exist to assign a unique address to each internet-connected device.[11] Therefore, the dynamic system has been adopted, in which each Internet Service Provider (ISP) is assigned a pool of IP addresses, which they assign to computers on an as-needed basis (i.e. whenever a customer requests internet access).[12] This means that a computer could be assigned a new IP address every time it is used to access the internet.[13] Therefore, most IP addresses do not identify an individual machine, but rather only the machine using that IP address at a specific time. In practice there is no way to tell if an IP address is dynamic or static on its face.[14]

Determining the identity of a machine through an IP address is also complicated by Network Address Translation (NAT), a protocol designed to further increase the availability of IP addresses.[15] When NAT is employed, the ISP assigns an IP address to a customer's central router or modem, which then creates a network of private IP addresses for every machine accessing the internet through that point.[16] By utilizing NAT a customer can connect multiple devices to the internet through a central router using a single IP address.[17] When this protocol is used, the IP address that is transmitted through the internet does not identify the single machine being used, but rather the router through which that machine is connected to the internet.

---

[10] *Id.*
[11] *Id.*
[12] *Id.* at 900-01.
[13] *Id.*
[14] *IP Addresses and the Data Protection Act*, OUT-LAW.COM (March 2008), https://www.out-law.com/page-8060. [https://perma.cc/U5VS-G6ML].
[15] SEVERANCE, *supra* note 4, at 47-8.
[16] *Id.*
[17] *Id.*

IP addresses generally do not identify a single machine (let alone a single person). At best an IP address must be first correlated to its time of use, and then cross-referenced with ISP customer records to determine to which customer account it was assigned. This still may not be enough to identify the machine in use, however. If the machine is part of a network utilizing NAT, the IP address will only point to the router accessing the internet, and the machine in question could be any of a number on that network. Additionally, it is important to remember that IP addresses do not refer to individual persons, but rather identify machines alone. Therefore, even when narrowed to a specific machine, an IP address cannot identify the user of that machine - the "butt in the seat" as it were.

III. WHAT IS PII AND HOW DO IP ADDRESSES RELATE?

The definition of PII is not easy to pin down. There are some universal examples of what constitutes PII, such as a name or physical address, but depending on the jurisdiction or activity in question, the definition can vary widely, or even be non-existent. Two major jurisprudential traditions have arisen regarding the treatment of PII, which I will refer to as the U.S. and the E.U. models. These two models take unique approaches to defining and protecting PII, and how IP addresses fit into the equation.

1. How is PII defined? The U.S. Model

In the United States, PII is afforded no general protection, and there is no overarching legal definition of PII.[18] Definitions are almost entirely sector specific, and are spread among various statutes related to specific activities.[19] In areas in which a statutory definition exists,

[18] McIntyre, *supra* note 1, at 902.
[19] *Id.*

the U.S. model tends to define PII by providing a list of examples of what is to be considered PII.[20] An example of this would be the definition of "record" included in the Privacy Act of 1974:

> [. . .] "record" means any item, collection, or grouping of information about an individual . . . including but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph . . . [21]

These definitions can vary between different statutes, but essentially have the same effect. If a piece of information contains some form of identifier – actually listed or substantially similar to the examples – that ties the information to the person to whom it relates, it is PII. These statutes also generally propound what requirements and restrictions are placed on handlers of such PII.[22]

In areas where a statute has not set out a definition of PII, it is left to private parties to define what PII is and what responsibilities the parties have regarding such.[23] This definition is most often accomplished through company privacy policies, which set out how customers' information is to be handled.[24] However, unless a business

---

[20] Frederick Lah, *Note: Online and Locational Privacy: Are IP Addresses "Personally Identifiable Information"?*, 4 I/S J. L. & POL'Y FOR INFO. SOC'Y 681, 684 (Winter 2008/Winter 2009).
[21] 5 U.S.C. § 552(a)(4) (2012).
[22] *See* 15 U.S.C. § 6502.
[23] Lah, *supra* note 20, at 684-85.
[24] As an example, Dyn, Inc., a domain name and internet management service provider, addresses personal information thusly:
"Any time you use Dyn's Sites or Services, information is generated. Some of this information is considered 'Personal Information,' meaning information that either directly identifies you individually (like your name, address, email, or billing information) or could reasonably be used to identify you in combination with other data.

operates in a sector which requires it to protect or otherwise specifically handle PII, there is no legal obligation for a company to contemplate such a definition.

As might be expected, some U.S. statutes contemplate the status of IP addresses as PII, and some do not. For instance, the Privacy Act of 1974, quoted above, does not expressly contemplate IP addresses. However, other privacy statutes, such as HIPAA and COPPA, do contemplate the status of IP addresses.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is perhaps the most well-known U.S. privacy statute.[25] HIPAA protects patient confidentiality in the healthcare context, and limits what information healthcare providers may provide to third parties regarding individuals.[26] As part of the requirements for releasing certain health records, HIPAA regulations require that a number of personal identifiers be scrubbed from any disclosed documents.[27] The regulations attached to HIPAA specifically include IP addresses in their definition of PII.[28] However, as this is an extremely sector specific statute, the protections it affords are limited, specifically to protecting patient information possessed by healthcare actors.[29]

Other information is considered 'Anonymous Information,' meaning information that does not directly identify, and cannot reasonably be linked with other data to identify you individually." DYN, INC., http://dyn.com/legal/dyn-privacy-policy/ (last modified Aug. 29, 2017) **[**https://perma.cc/NZR2-7NUY**]**.

[25] Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996).

[26] *The HIPAA Privacy Rule*, U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES, https://www.hhs.gov/hipaa/for-professionals/privacy/ (last visited Mar. 25, 2017) **[**https://perma.cc/93R5-TCZV**]**.

[27] 45 C.F.R. § 164.514(b)(2)(i)(O) (2017).

[28] *Id.*

[29] 45 C.F.R. § 160.402.

Another specific statute which protects IP addresses as PII is the Children's Online Privacy Protection Act of 1998 (COPPA).[30] COPPA was enacted to regulate how websites aimed at, or knowingly used by, children collect information about those children.[31] Therefore, COPPA only applies to these particular website operators, and only in regards to the information of those under thirteen years of age.[32] Although the original statutory definition of personal information under COPPA did not include IP addresses, it included a provision for "any other identifier that the Commission determines permits the physical or online contacting of a specific individual."[33] This provision was used to expand the definition of personal information to include "persistent identifier[s] that can be used to recognize a user over time and across different Web sites or online services.[34] Such persistent identifiers include, but are not limited to, "a customer number held in a cookie, *an Internet Protocol (IP) address*, a processor or device serial number, or unique device identifier."[35]

Incorporating IP addresses into COPPA's personal information definition renders them subject to the various restrictions of the statute. These include requirements that the website give notice of what information is being collected, and how it is to be used and disclosed; receive verifiable parental consent to collect such information; and "maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children."[36]

---

[30] 15 U.S.C. §§ 6501-6505.
[31] *Id.* at § 6502.
[32] 15 U.S.C. §§ 6501-6502.
[33] *Id.* at § 6501(8)(f).
[34] 16 C.F.R. § 312.2.
[35] *Id.* (emphasis added).
[36] 15 U.S.C. § 6502.

Beyond these statutory designations, courts in the U.S. have been loathe to interpret other definitions of PII as including IP addresses. A leading federal case on this point is *Klimas v. Comcast Cable Communications, Inc.*[37] In this case, the plaintiff alleged that Comcast violated §551(a) and (b) of the Cable Communications Policy Act of 1984 by collecting the PII of subscribers.[38] Specifically their IP addresses and the URLs of websites they visited.[39] The plaintiff alleged that Comcast had the ability to correlate this information with its subscriber list, and therefore identify the web-surfing habits of any subscriber.[40] The plaintiff characterized these IP addresses and URL logs as PII that should be protected under the statute.[41]

The court dismissed the case on the grounds that Comcast's ISP service did not fall under the definition of cable service in the statute, and therefore data collection through such was not within the contemplation of the statute.[42] However, the court finished its analysis by stating that, even if the Cable Act provisions had applied, the statutory definition of "personally identifiable information" would not include records of aggregate data which do not identify particular persons.[43] Therefore, unless Comcast had taken the extra step to actually correlate the collected IP addresses with its list of subscribers, the IP addresses would not identify particular persons. Thus, the court adopted the notion (albeit in dicta) that IP addresses in solitude are not PII, and do not fall

[37] *Klimas v. Comcast Cable Communications, Inc.*, 465 F.3d 271, 271 (2006).
[38] *Id.* at 273.
[39] *Id.* at 274.
[40] *Id.*
[41] *Id.*
[42] *Id.* at 276.
[43] *Id.* at 280.

under the protections of such unless they are coupled with other information.[44]

Courts have also refused to interpret definitions of PII as including IP addresses in non-statutory, contract claims. In *Johnson v. Microsoft Corp.*, Microsoft's definition of "personally identifiable information" under an end user license agreement ("EULA") came into question.[45] The EULA did not expressly include IP addresses, and Microsoft argued that the definition should not be interpreted to include IP addresses.[46] The court, partly relying on *Klimas*, found that Microsoft's interpretation was reasonable, stating that for information "to be personally identifiable, it must identify a person. But an IP address identifies a computer, and can do that only after matching the IP address to a list of a particular Internet service provider's subscribers. Thus . . . an IP address is not personally identifiable."[47]

Efforts to revamp the U.S.'s sector-specific framework have been advanced, but have not been successful. In 2010, Rep. Bobby Rush (D - IL) introduced H.R. 5777, a bill relating to the handling of consumer information by companies participating in interstate commerce.[48] This bill included a broad definition of what entities would be covered, to include any "person engaged in interstate commerce that collects or stores data containing covered information or sensitive information," with exceptions for companies which can show that they store and collect covered information of a limited number of individuals, do not store sensitive information, and do

---

[44] *Id.*
[45] *Johnson v. Microsoft Corp.*, No. C06-0900RAJ, 2009 U.S. Dist. LEXIS 58174, at *10 (W.D. Wash. June 23, 2009).
[46] *Id.* at *11-12.
[47] *Id.* at *12-13.
[48] BEST PRACTICES Act, H.R. 5777, 111th Cong. (2010).

not use covered information to study the behavior of individuals as their primary business.[49]

H.R. 5777 defined two categories of protected information: "covered information," and "sensitive information."[50] Sensitive information was defined as information relating to an individual's health, religion, income, and sexual orientation; while covered information included more generic identifiers such as physical and e-mail addresses, names, and phone numbers.[51] In addition to these common forms of information, the text expressly identified IP addresses as "covered information."[52] However, the bill was sent to committee in 2010, and never made further progress.

There is no clear answer as to whether IP addresses constitute PII in the United States. The most that can be said is, it depends. Generally, the determination will be sector-specific, and expressly outlined in the definitions of specific statutes, such as HIPAA and COPPA. However, without such an express designation, courts are unlikely to define IP addresses as PII.

2. IP Addresses as PII in the European Union

The legal tradition regarding PII in the European Union has been the polar opposite of that in the U.S. The "right" to data privacy has long been recognized in the EU, and protected by broad legislation.[53] Since 1995, EU member states have been subject to the Data Protection

[49] H.R. 5777 at § 2(3).
[50] *Id.* at §§ 2(4), (8).
[51] *Id.*
[52] *Id.* at § 2(4)(A)(vii).
[53] *See* Charter of Fundamental Rights of the European Union art. 8, 2010 O.J. C 83/02; *see generally* Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 O.J. (L 281) 1.

Directive (DPD) and, since 2016, its replacement, the General Data Protection Regulation (GDPR).[54] These two laws are identical in many ways, but the GDPR changes the legal landscape in a few key aspects, the most important of which for our purposes is the definition of personal data. Under the DPD, every member-state interpreted the meaning of the rules in its own way, including what was covered under the Directive's definition of personal data. The GDPR, on the other hand, sets out a clear and strict definition which is no longer up for interpretation.

The overarching definition of personal data under the GDPR stands in contrast to the patchwork definitions of PII found in U.S. law. The GDPR definition is essentially identical to the definition under the replaced DPD, and reads[55]:

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

When data falls under this definition, the GDPR requires that it be processed in accordance with various data protection principles.[56] These include principles

---

[54] *See generally* Parliament and Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *supra* note 53; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1.
[55] GDPR, *supra* note 54, at art. 4(1).
[56] *Id.* at Chapter II.

regarding an individual's rights to have his data deleted or corrected, how that data may be used, and most notably, how that data must be protected. In practice, this requires companies and organizations to implement an effective data protection system to protect data from being breached, damaged, or destroyed.

As can be seen above, the definition of PII in the GDPR does not make mention of IP addresses; this was also true when the DPD was operative.[57] However, during the DPD era, the Article 29 Working Party[58] expressly stated that IP addresses should be considered PII, and be subject to the protections of the directive.[59]

In its Opinion 4/2007 on the concept of personal data, the Working Party provided an element by element analysis of the definition of personal data.[60] It is important to note that this report was merely the opinion of the Working Party, and was not binding on the member states.[61] Nevertheless, the Working Party included IP addresses as an example of information which relates to an identifiable person.[62] The Working Party reasoned that, because local area network managers and ISP providers could identify internet users by their IP address using

---

[57] GDPR, *supra* note 54, at art. 4(1); DPD, *supra* note 53, at art. 2 para. (a).

[58] The Article 29 Working Party is a panel convened under the DPD, made up of representatives from all member-states as well as representatives from the European Commission, and tasked with providing expert advice on data protection issues, and the DPD, to the EU.

[59] Peter Schaar, *Opinion 4/2007 on the concept of personal data*, Article 29 Data Protection Working Party WP 136 1, 4 (2007), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf (accessed Apr. 20, 2016) [https://perma.cc/UHV2-FLGU].

[60] *Id.*

[61] *Id.* at 3.

[62] *Id.* at 16-17.

"reasonable means," IP addresses "related" to identifiable natural persons, and were therefore personal data.[63]

The opinion also left room for scenarios where IP addresses might not constitute personal data, such as computers in internet cafes, used transiently by many people.[64] However, the Working Party pointed out that there is generally no clear way of telling whether an IP address belongs to such a computer, and therefore all IP addresses should be treated as personal data.[65]

The opinion of the Working Party was largely adopted by a decision of the European Court of Justice (ECJ) in 2011. In *Scarlet v. SABAM*, the ECJ was asked to give a preliminary ruling on whether an ISP could be required to provide a filtering system, at its own cost, for the purpose of stopping the transmission of files infringing on certain intellectual property rights.[66] The court determined that such a requirement would not be allowable for a variety of reasons, including that such a system would require the provider to undertake a "systematic . . . collection and identification of users' IP addresses . . . ."[67] The court said that these addresses are "protected personal data," and allowing such a collection would infringe on customers' fundamental right to the protection of personal data.[68]

However, officials in some member states have expressed opinions differing from the Working Party's conclusion.[69] In 2001 then-UK Information Commissioner Elizabeth France opined that IP addresses were likely not

---

[63] *Id.*
[64] *Id.* at 17.
[65] *Id.*
[66] C-70/10, *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 2011, E.C.R. I-12020 to I-12021.
[67] *Id.* at I-12027.
[68] *Id.*
[69] IAN J. LLOYD, INFORMATION TECHNOLOGY LAW §5.6 (4th ed. 2004).

PII. She stated that, because it is difficult to determine if an IP address is static or dynamic, ". . . the scope for using IP addresses for personalized profiling is limited."[70] She further stated that IP address would likely not fall under the protection of the UK Data Protection Act unless the controller held or had public access to other forms of PII relating to the individual using the IP address.[71]

This era of cognitive dissonance between the Working Party and member states appears to be at an end with the adoption of the GDPR last year.[72] As the DPD was only a directive, member states had freedom to interpret its provisions quite liberally.[73] However, because the GDPR is a regulation, it is wholly binding on the member states, and meant to be interpreted uniformly.[74] As there is essentially no difference in the language, intent, or meaning of the DPD and GDPR as it comes to defining personal data, it is safe to assume that the guidance previously provided by the Working Party is just as applicable now as it was under the DPD. Therefore, it appears that IP addresses will be treated EU-wide as PII.

---

[70] It is important to note that the U.K. was a member of the EU in 2001. As of 2017, the process of the U.K.'s exit from the EU has begun, and upon exit, the GDPR will no longer be binding on that country.
[71] *IP Addresses and the Data Protection Act*, OUT-LAW.COM (Mar. 2008), https://www.out-law.com/page-8060. [http://perma.cc/BE37-JAEM].
[72] The GDPR was adopted on April 14, 2016.
[73] Zack Gross, *8 Ways EU GDPR Differs From the EU Data Protection Directive*, CLOUDLOCK (May 12, 2016), https://www.cloudlock.com/blog/eu-gdpr-vs-data-protection-directive/. [http://perma.cc/LC2A-D7Z2].
[74] *Id.*

IV. WHY IP ADDRESSES SHOULD NOT BE CONSIDERED PII

Although there is a trend toward designating IP addresses as PII, as evidenced by the Working Party's opinion, the failed BEST PRACTICES Act, and the isolated instances where U.S. law has so defined them, IP addresses are inherently different from other, more traditional forms of PII, and should not be granted the same level of protection. First, the dynamicity and indefiniteness of IP addresses precludes them from identifying, or making identifiable, persons. Second, the disclosure of IP addresses to third parties does not present as significant a risk to individuals' privacy as does the disclosure of traditional forms of PII. Finally, defining IP addresses would impose a significant burden on businesses, inconsistent with the actual dangers an individual faces if his IP address is revealed.

A. IP Addresses Do Not Identify, or Make Reasonably Identifiable, Persons

When all the various definitions are parsed, the basic essence of PII is information that identifies or makes a person reasonably identifiable. Because IP addresses do not fit in either of these categories, they do not fit the traditional definition of PII and therefore should not qualify for the same protection.

First, IP addresses are never connected to a person, and therefore cannot *identify* such. IP addresses are not unique identifiers such as Social Security or driver's license numbers, which are directly connected with singular persons.[75] Thus, if IP addresses are to be considered PII at

[75] Driver's license numbers sometimes present an interesting case in both being an identifier themselves, and allowing other PII to be discovered without any other information or correlation. New

all, they must somehow make a person *reasonably identifiable*. However, this is just not the case. IP addresses, although similar in some ways to traditional PII, also bear striking differences which illustrate why they do not deserve the same level of protection.

1. Dynamicity

The first major difference between IP addresses and traditional PII is their dynamicity. As previously explained, the dynamic addressing system necessary for the Internet Protocol to function requires an internet-connected machine's IP address to frequently change.[76] This dynamicity adds a level of separation between IP addresses and individuals not seen in other forms of PII, and renders the value of the information a third party could amass minimal.

Traditional forms of PII are largely static, without any level of temporal separation from their data subject. For instance, birthdates, names, and Social Security numbers are all unchanging. They stay with a person for life, and can be continuously used to identify an individual.[77] Not *all* forms of traditional PII are so static; physical addresses, and phone numbers can change. For instance, a person can move residences, or change phone lines. However, when a person obtains an address or phone number, it is generally for an indefinite period, usually of a

Hampshire, for example, formulates license numbers based off the issuee's birthdate and first and last names.

[76] *Supra* Part I.

[77] There are exceptions to this. Obviously, names can be legally changed, and new Social Security numbers can be assigned at request, for instance after an individual's identity has been stolen.

long duration.[78] [79] Further, when one decides to change any of these identifiers, it is done quite deliberately, and individuals generally inform others of the changes in order to remain in contact, and to continue receiving services - such as mail, electricity, and other necessities.

IP addresses are certainly not static, like Social Security numbers or birthdates; nor are they deliberately retained for prolonged periods of time, such as a physical address or phone number. They are randomly assigned by ISPs whenever a device connects to the internet, and may change each and every time this occurs. Internet users generally have no control over what their machine's IP address is, or when they are assigned a new one. This inherent mutability of IP addresses renders them distinct from traditional PII, in that they may change at the drop of the hat, without any action by the user, and are only connected to a certain subscriber for a very limited period.[80] This constant re-addressing means that before

---

[78] U.S. Census survey results show that the median length of time that respondents had resided in their current homes was 5.2 years. Kristin A. Hansen, U.S. CENSUS BUREAU, SEASONALITY OF MOVES AND DURATION OF RESIDENCE 4 (1998) https://www.census.gov/sipp/p70s/p70-66.pdf .[http://perma.cc/225R-9SHL].

[79] 47 U.S.C. § 251 allows for, and requires, the porting of customer phone numbers between telecommunications providers, and data has shown that the average American now retains the same cellular phone for 26 months. (the length of time that a user keeps their phone number is likely much longer than this 26 months, as that number only indicates when the user changes *hardware* and not the underlying service) *See* Daniel B. Kline, *How Often Does The Average American Replace His Or Her Smartphone?*, THE MOTLEY FOOL (July 15, 2015 10:03 AM), https://www.fool.com/investing/general/2015/07/15/how-often-does-the-average-american-replace-his-or.aspx. [http://perma.cc/7STQ-HQAP].

[80] *How Long Does an IP Address Stay Attached to a Home or Business?*, EL TORO, http://eltoro.com/how-long-does-an-ip-address-stay-attached-to-a-home-or-business/ (last visited Feb. 14, 2018). [http://perma.cc/2RUU-UEAY].

any attempt to identify an individual through his IP address can even begin, that IP address must first be connected with the *exact* time of its use.

This dynamicity not only provides a temporal separation increasing the difficulty with which IP addresses may be connected to an individual, but also reduces the usefulness of IP addresses in discovering personal information about an individual utilizing that IP address. The UK information commissioner has commented on how dynamic IP addresses are difficult to use in building a personalized profile on an individual, and that dynamic IP addresses likely would not fall under the purview of the UK Data Protection Act 1998 (the UK's data protection scheme adopted after the inception of the DPD). This guidance was memorialized in a report issued by the Information Commissioner's Office in May 2007.[81]

This lack of usefulness in building any personalized profile on an individual is exacerbated by the changing way in which people are computing. With the advent of smartphones and tablets, less and less internet traffic is coming from home-based PCs. Studies have shown that year-over-year, desktop PC usage is on a downward trend, down as much as 9.5% in December, 2015.[82] At the same time, use of mobile devices is on the rise. In fact, 20% of people aged 18-34 reported not even using a desktop PC at

[81] UK INFORMATION COMMISSIONER'S OFFICE, DATA PROTECTION GOOD PRACTICE NOTE (2003) http://webarchive.nationalarchives.gov.uk/20100402134332/http:/ico.gov.uk/upload/documents/library/data_protection/practical_application/collecting_personal_information_from_websites_v1.0.pdf. [http://perma.cc/GL57-CGFF].

[82] Ryan Whitwam, *ComScore: Computer Usage Falls as 20% of Millennials go Mobile-only*, EXTREMETECH (Apr. 19, 2016 3:25 PM), https://www.extremetech.com/computing/226867-comscore-computer-usage-falls-as-20-of-millennials-go-mobile-only. [http://perma.cc/8LZR-5DGN].

all, instead relying entirely on mobile devices for their internet needs[83].

This reliance on mobile devices compounds the dynamicity issue for anyone attempting to identify an individual through an IP address. When an individual is using a mobile device to connect to the internet, they are often, as the name suggests, mobile. This means that the chances of the user's IP address changing whenever they connect to the internet are even higher, as they are often changing access points, each of which is a separate entity in relation to the ISP, also being assigned and reassigned IP addresses. These access points are often public, bear no relation to the individuals utilizing them, and if the IP address assigned from these points was correlated with subscriber data, would not point in any way towards the user.[84]

2. Indefiniteness

The second major difference between IP addresses and traditional PII is their indefiniteness. For a piece of information to be personally identifiable, it must refer to a sufficiently discrete number of people that an individual may be reasonably identified. Some forms of PII are unique and identify only one individual, such as Social Security numbers. Physical addresses, phone numbers, and birthdates are all examples of indefinite PII; none of these forms identify a single individual. Physical addresses can identify any individual who resides at a certain place; phone numbers can identify the users of a certain phone line; and birthdates can identify all persons born on a certain day.

---

[83] *Id.*

[84] Rather, it would only indicate the subscriber information for the owner of the network which the individual is connecting to (i.e. a business, library, or other place of public accommodation).

IP addresses are certainly not unique identifiers. They are not unique to single individuals, and they do not even directly relate to persons at all, but machines. Even if one successfully correlates an IP address to its time of use, and to the subscription account to which it was assigned at that specific time, that correlation does not identify the actual individual accessing the internet at that time.[85] Private internet subscriptions, although associated with a single account holder, are generally shared by an entire household with all members, and any visitors, accessing the internet through the same IP address. Additionally, with the rise of wireless technologies, access to many internet subscriptions is not limited to the discrete members of a household. As many as 51% of wireless networks may not be password protected[86], and are therefore open to use by anyone within range of the signal.[87] Public wireless access points are becoming increasingly popular as well. These networks are *designed* to be open to any passers-by and correlation of an IP address with the subscriber information held by the ISP can provide no information relating to any identifiably discrete group of individuals.

Other forms of PII do have levels of indefiniteness, but they do not rise to that of IP addresses. Birthdates, for example, can identify the entire class of people born on a specific date; however, this class never changes, whereas IP addresses are constantly reassigned to new subscribers. Phone numbers may be shared between individuals, but users have the ability of being identified by simply calling

---

[85] In fact, as mentioned *supra* in Part I, it may not even identify the machine in use if the IP address is assigned to a router using NAT.

[86] Elinor Mills, *The Unvarnished Truth about Unsecured Wi-Fi*, CNET (Nov. 1, 2010 4:00 AM PDT), https://www.cnet.com/news/the-unvarnished-truth-about-unsecured-wi-fi/. [http://perma.cc/G24Z-YR9Q].

[87] As of the time of this writing, the author was able (at home) to detect two unsecured wireless networks to which he was able to connect, in a fairly rural neighborhood.

the number and asking for the person the number is allegedly tied to. Phone numbers also differ in that they tend to be much more permanent, and are consciously used by individuals as a means of direct contact.[88]

Putting aside the issue of public internet access points, physical addresses are perhaps the closest PII in form to IP addresses in terms of identifying a person. When an IP address is correlated with subscriber data in an attempt to identify a person, what is really happening is that the number of persons that IP address could relate to is being reduced to the class that accesses the internet at the address connected to the account. Likewise, when an address is used to identify a person, the address is merely reducing the number of potential individuals to those residing at that address. On their face, these might appear to be nearly identical situations. But the group that shares a residence, and the group that uses the internet access point associated with a residence are two very different things. Where other commentators have gone wrong is in assuming an internet access point is only shared by those whom also reside at that address.[89] However, this is often not the case,

---

[88] Studies have indicated that the average time that consumers keep cell phones is 26.5 months, greater than two years. The average length of time that phone numbers are retained by consumers is likely much higher, as many consumers simply replace their hardware when purchasing a new phone, rather than a whole new service. Additionally, with the ability to port numbers between carriers, many who do switch their entire service likely hold on to their previously existing number for convenience. Roger Entner, *2014 US Mobile Phone Sales Fall by 15% and Handset Replacement Cycle Lengthens to Historic High*, RECON ANALYTICS (Feb. 10, 2015), http://reconanalytics.com/2015/02/2014-us-mobile-phone-sales-fall-by-15-and-handset-replacement-cycle-lengthens-to-historic-high/.[http://perma.cc/VW42-SE8J].

[89] JD Sartain, *Can Your IP Address Give Away Your Identity to Hackers, Stalkers and Cybercrooks?*, NETWORK WORLD (July 16, 2013 10:59 AM PT), http://www.networkworld.com/article/2168144/malware-

and the actual class identified by an IP address connected to a private internet access point may actually be much larger than just the individuals residing at that residence. For instance, access is often shared with any visitors, access may have been granted to neighbors, access may be completely unrestricted, and there may even be unauthorized users who have gained access despite a password protection.

3. Risk of Harm

Finally, the disclosure or discovery of IP addresses does not pose the same risks to individuals as does the disclosure or discovery of traditional forms of PII. The rationale behind protecting PII is largely protecting a person's privacy. However, the privacy dangers stemming from the misuse of an IP address are minimal as compared to traditional forms of PII.

Disclosure of traditional forms of PII opens an individual up to numerous risks of potential harassment or harm simply not possible from the disclosure of an IP address. For instance, if an individual's physical address is disclosed, that person can become the target of vandalism, or stalking; the disclosure of a phone number can lead to harassment; disclosure of an email address can open the door to unwanted spam; and the disclosure of a birthdate or Social Security number can lead to identity theft or other forms of fraud.

The disclosure of an IP address can lead to none of these things. IP addresses do not expose the exact geographical location of the machine they are tied to, eliminating the concern over physical vandalism or stalking. Because IP addresses are so dynamic, they do not allow for any prolonged harassment through electronic interference. Finally, IP addresses are in no way tied to an

---

cybercrime/can-your-ip-address-give-away-your-identity-to-hackers--stalkers-and-cybercrooks-.html. [http://perma.cc/YB3A-82W3].

individual's bank accounts, credit cards, or other documents that are potential targets for identity thieves.

What an IP address can divulge are aspects of an individual's personal life: his browsing habits, and potentially other personal attributes, including his health condition, sexual predilections, or political beliefs. These are certainly things that can harm an individual if disclosed, but in reality the risk of this information being tied to an individual through an IP address are slim. The issue is again the dynamicity of IP addresses, as well as the dynamicity of how people use the internet. Because a user's IP address can change every time that a user logs on to the internet (and necessarily does when the user changes access points) the user's browsing history may effectively "reset," forcing any interested third party to restart the process of building a profile. Even if an individual were to utilize a single IP address for an extended period, it is likely that that user is sharing his IP address with others, whether that connection is a private home account shared by all the residents and guests, or a public access point open to anyone in the area. This means that any profile that may be created through that IP address is likely to not be an accurate depiction of an individual's internet use, as it will be practically impossible to sift what web traffic is attributable to what user.

B. Cost/Liability to Business Owners

Beyond any concerns that might arise as to whether IP addresses actually meet the definition of PII, declaring that IP addresses are PII presents economic concerns that also deserve contemplation. For such a declaration to have any benefit, real or perceived, it must come along with penalties for parties which fail to protect IP addresses, in

reality – businesses with an online presence.[90] Imposing such a mandate on businesses would levy unreasonable costs and risks of liability on businesses, not justified by the minimal extra privacy afforded to consumers.

This is an age of regulation, and many would say overregulation. Businesses today face an ever increasing regulatory state, promulgating over 2,500 new regulations per year.[91] This increasingly large body of law has become ever more burdensome for businesses, especially small businesses, to navigate, and the cost has similarly risen.[92] Recent studies have indicated that the regulatory burden on small businesses in today's market exceeds $10,000 per employee.[93] For a small business with only three employees, that amount is equal to the cost of two additional minimum wage workers.[94]

This is also an age where internet presence is of the utmost importance to successful companies. Studies have shown that as many as 81 to 97% of consumers research

---

[90] Any ability to create such a broad rule would likely rely on Congress's Interstate Commerce Clause power – as was the failed Best Practices Act – thereby making any regulation effective against those doing business across State lines.

[91] 20,462 new regulations were introduced between 2009 and 2015. James Gattuso & Diane Katz, *Red Tape Rising 2016: Obama Regs Top $100 Billion Annually*, THE HERITAGE FOUNDATION (May 23, 2016), http://www.heritage.org/government-regulation/report/red-tape-rising-2016-obama-regs-top-100-billion-annually?_ga=1.249263681.779512437.1488551738. [http://perma.cc/54ZT-JMTK].

[92] Compliance costs rose $22 billion between 2015 and 2016. *Id.*

[93] Scott Shane, *To Help Small Business, Cut Regulation*, ENTREPRENEUR (Jan. 10, 2014), https://www.entrepreneur.com/article/230727. [http://perma.cc/F6QE-FFNF].

[94] Calculated at the federal minimum rate of $7.25 per hour, at 2,080 hours per year.

products and services on the web before purchase.[95] Companies who forego the process of creating a webpage thereby stand to lose eight or nine of every ten potential customers. Despite this, the number of small businesses without an online presence is staggeringly high. Various studies have indicated that only approximately 50% of small businesses have a website, and of those without a website, only 12% had something similar, such as a Facebook page.[96] When asked about why they chose not to publish a website 21% said it was because of a lack of expertise, and 20% because it was too expensive.[97]

Defining IP addresses as PII that needs to be protected would impose an unnecessary additional barrier to entering the online marketplace for these companies. Every "mom and pop" with a webpage listing its hours and address would need to institute a data protection plan ensuring that its visitors' IP addresses were secure.[98] If many of these companies lack the technical expertise to even create a website, they likely lack the technical expertise to understand how IP addresses work and how to protect them. Further, if many of these companies are unable to afford the generally low cost of operating a

---

[95] *Lack of Websites Common Pitfall for Small Businesses*, PITTSBURGH POST-GAZETTE (Jan. 6, 2015 12:00 AM), http://www.post-gazette.com/business/pittsburgh-company-news/2015/01/06/Lack-of-websites-common-pitfall-for-small-businesses/stories/201501060018; [http://perma.cc/5YBB-VPGM].

[96] Tess Townsend, *Many Small Businesses Have Little to No Online Presence*, INC. (Sept. 16, 2016), http://www.inc.com/tess-townsend/small-business-survey-godaddy-websites.html. [http://perma.cc/7UTB-AJKC].

[97] *Id.*

[98] IP addresses are collected by web servers every time that an individual visits a website, and therefore even if a website is nothing more than a single informational page, visitors' IP addresses are collected and stored by the website operator.

website as of now, the added cost of compliance would certainly put a website out of economic possibility.[99]

Beyond the constant carrying cost these businesses would face for ensuring IP privacy, they would also have to account for potential legal liability should their security protocols fail. For instance, if a broad-based IP address protection was instituted, any legislation would likely resemble other internet privacy statutes, such as COPPA, in that it would include penalties for failing to comply. This liability will require any company operating a website to either carry insurance for any breach or compliance failure, or bear the risk of any potential enforcement action in the future. These are all potential costs that a company must consider before opening itself to liability.

V. A POSSIBLE SOLUTION TO PROTECTING IP ADDRESSES

As IP addresses do not make persons even arguably identifiable unless they are correlated with other subscriber data, it does not make sense to require their protection where they are held in isolation (such as the visitor log of a website). Even if IP addresses were held in conjunction with traditional forms of PII, protection of IP addresses would essentially be redundant, so long as any other PII with which they might be correlated are properly protected. Therefore, adding IP addresses to the definition of PII is unnecessary to adequately protect an individual's privacy.

Despite this, some may still be concerned about their online habits being discovered or tracked through their IP address(es). There is room for a solution that will allow

[99] Average domain name and web hosting costs per year are between $50 and $1,200. KeriLynn Engel, *How Much Does a Website Really Cost?*, WHOISHOSTINGTHIS? (July 29, 2014), http://www.whoishostingthis.com/blog/2014/07/29/website-cost/. [http://perma.cc/WQ5U-28WS].

individuals to feel that any perceived privacy risks are mitigated and not place an undue burden on businesses to protect such data. As discussed, some of the main concerns keeping small businesses from creating websites are the cost, and a lack of technical expertise. Therefore, if IP addresses can be adequately protected at a point where the controller has the necessary means and expertise that such protection would not be prohibitive, an individuals' privacy concerns can be ameliorated, and businesses concerned with cost or lack of expertise can be free to operate websites without the costs of protection or risks of liability.

A. The Proposed Solution

The logical solution would be to protect IP addresses, and other PII, at the ISP level, where the necessary correlation must occur for any useful information to be obtained from an IP address. If ISPs were required to protect subscriber IP addresses and other PII, this correlation simply could not occur. If a regulation were to be imposed which barred ISPs from disclosing any information about customer IP addresses, or other PII, then an individual would essentially be wholly protected from any risk of being identified through his IP address. If a third party were to come to an ISP with an IP address seeking the connected subscriber data, the ISP would be barred from providing any information. The same would be true in reverse; if a third party came to an ISP with a subscriber's name and requested any IP addresses assigned to that subscriber's account, the ISP would similarly be barred from providing any IP addresses and times of use.

Implementing this protection regime at the ISP level also resolves any potential concerns of business-owners wishing to have an online presence, but concerned about the cost or liabilities that a data protection mandate would incur. By their very nature, ISPs have the technical

expertise to understand IP addresses, how they work, and what actions would be necessary for adequate protection. Additionally, cost concerns are much less of an issue when such requirements are levied on ISPs, rather than broadly across website operators of all sizes.[100] Costs of regulations affect larger companies to a significantly smaller scale than small companies, and ISPs are anything but small.[101]

B. The Adopted Compromise

A potential solution to the problem, largely along these lines, has already been implemented, albeit briefly. The Federal Communications Commission (FCC) recently adopted new rules which appear to have struck a middle ground on IP address protection, targeted at the ISP level. In October 2016, in accordance with Section 222 of the Communications Act, the FCC approved new rules regarding what ISPs can do with subscriber information.[102]

Under this new framework, ISPs are required to handle, maintain, and protect PII in many of the same ways companies are required to under the GDPR in Europe.[103]

---

[100] Costs of complying with federal regulations are 36% higher for small businesses than large businesses. Courtney Rubin, *Federal Regulations Costly for Small Businesses*, INC. (Sept. 27, 2010), http://www.inc.com/news/articles/2010/09/federal-regulations-cost-small-businesses-more-than-large-ones.html. [http://perma.cc/9F2L-NV9B].

[101] Two of the largest ISPs in the U.S., AT&T and Comcast, have 254,000 and 164,000 full-time employees, respectively. YAHOO! FINANCE, https://finance.yahoo.com/quote/T/profile?p=T (last visited Feb. 17, 2018); YAHOO! FINANCE, https://finance.yahoo.com/quote/CMCSA/profile?p=CMCSA (last visited Feb. 17, 2018). [http://perma.cc/UM23-CAWQ].

[102] FEDERAL COMMUNICATIONS COMMISSION, Report and Order: In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16-106 (Nov. 2, 2016).

[103] *Id.* at ¶¶ 7-10.

The rules discuss many of the same principles of openness, customer control, notification, and protection as the GDPR.[104] These rules delineate an opt-in/opt-out scheme which requires ISPs to not release sensitive personal information of customers unless the customer specifically opts-in to allow such disclosures.[105] Other personal information that is not deemed "sensitive" is disclosable, unless the customer specifically opts-out.[106]

IP addresses appear to be non-sensitive personal data under these rules and therefore are free to be disclosed by the ISP, unless the customer specifically opts-out of such disclosures.[107] The ISP is required to make a clear communication of all the ways in which it uses a customer's data, and also clearly communicate the ability to opt-out of such use or sharing.[108] If ISPs fail to comply with a customer's desire to opt-in, opt-out, or otherwise fail to properly protect a customer's information, these rules make them subject to civil damages and administrative fines.[109]

C. The Push-Back

With the election of the Trump administration in November 2016, the survival of this new protection

---

[104] *Id.*
[105] *Id.* at ¶ 9; 47 C.F.R. § 64.2004.
[106] FEDERAL COMMUNICATIONS COMMISSION, Report and Order: In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16-106 at ¶ 9; 47 C.F.R. § 64.2004.
[107] Kate Cox, *Final FCC Privacy Rule Won't Ban Pay-For-Privacy, Will Require Some Opt-Ins*, CONSUMERIST (Oct. 6, 2016 2:01 PM EDT) https://consumerist.com/2016/10/06/final-fcc-isp-privacy-rule-doesnt-ban-pay-for-privacy-does-require-some-opt-ins/ [http://perma.cc/RJT8-4DWY].
[108] 47 C.F.R. § 64.2003.
[109] 47 U.S.C. §§ 205, 206.

framework has come into doubt. With the administration change, Commissioner Ajit Pai, a vocal opponent of the regulation, has been promoted to the role of FCC Chairman.[110] Although these regulations were intended to go into effect on March 2, 2017, on March 1 Chairman Pai announced a stay order that effectively blocks the implementation of this new regulation.[111]

This stay order comes after significant pushback from ISPs over the new regulation. The major argument from ISPs against the regulation was that it produced an unfair imbalance in how internet actors are required to protect internet user privacy.[112] For instance, other large internet actors, such as Google, Microsoft, and Apple are not required to abide by the new regulations, despite the fact that they collect and share visitor data as well.[113]

On April 3, 2017, the President signed into law Senate Joint Resolution 34 (2017-18), giving this stay order permanent effect.[114] The Resolution constitutes a total disapproval of the new rules adopted by the FCC, and its adoption bars their implementation.[115] This means that the current protection of IP addresses as PII returns to the

---

[110] *See* Ajit Pai, *Dissenting Statement of Commissioner Ajit Pai Re:* Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, *WC Docket No. 16-106*, https://apps.fcc.gov/edocs_public/attachmatch/FCC-16-148A5.pdf [http://perma.cc/ZRM7-D5UU]. (Last visited Mar. 28, 2017).
[111] Buckley Sandler LLP, *FCC, FTC Issue Joint Statement on Broadband Data Security Regulation; Senate Resolution Introduced to Repeal FCC Privacy Rules*, LEXOLOGY (March 10, 2017), http://www.lexology.com/library/detail.aspx?g=b3cfd3d7-8268-4f05-bd5f-ef0005196698. [http://perma.cc/SW3G-CGLG].
[112] *Id.*
[113] These actors were not regulated by the new FCC rules, and their practices were still under the purview of the FTC's regulations which are not so restrictive.
[114] S.J. Res. 34, 115th Cong. (2017).
[115] *Id.*

status quo, and leaves us again in a gray area concerning their classification.

VI. CONCLUSION

IP addresses are simply not PII. They are connected to machines not people, and although they can be correlated with other data about individuals, that correlation cannot be made with any degree of certainty in order to unmask an individual's identity. This lack of certainty comes from the inherent dynamicity and indefiniteness of IP addresses, which render them distinct from traditional forms of PII.

Despite this disconnect, there is a strong belief among many that IP addresses should still be protected. However, IP addresses are eventually classified – either as PII or not – resolution on how, or if, they are to be protected is a question that does not appear to be one that will be resolved anytime soon, or without significant compromise. We have already seen an attempt at such an imperfect compromise, which ended in failure before it even took effect. What can be said with certainty is that, although foreign jurisdictions have fully and definitively adopted the position that IP addresses are PII, and U.S. law appears to have been moving in this direction in recent years, the new administration's strong position on deregulation seems to indicate that these movements will be rolled back, or completely stalled, for the near future.