Washington Journal of Law, Technology & Arts

University of Washington School of Law

VOL. 10 SUMMER 2014 NO. 1

CONTENTS

Washington Journal of Law, Technology & Arts

University of Washington School of Law

VOL. 10 SUMMER 2014 NO. 1

WASHINGTON JOURNAL OF LAW, TECHNOLOGY & ARTS
VOLUME 10, ISSUE 1 SUMMER 2014

THE EVOLVING LANDSCAPE OF TCPA CONSENT STANDARDS AND WAYS TO MINIMIZE RISK

Misa K. Bretschneider[*]

Cite as: 10 Wash. J.L. Tech. & Arts 1 (2014)
http://digital.lib.washington.edu/dspace-law/handle/1773.1/1387

ABSTRACT

Given the exponential growth in mobile phone usage, more businesses are adopting mobile communication strategies to engage with existing and potential customers. With 97% of all mobile marketing text messages being opened by their intended recipients, mobile text message marketing is both effective and lucrative. However, businesses must ensure that such messages comply with the Telephone Consumer Protection Act (TCPA), which generally prohibits sending unsolicited commercial text messages. Indeed, TCPA litigation has become the recent darling of class action lawyers due to uncapped statutory damages and is sure to increase with the heightened consent regulations promulgated by the Federal Communications Commission (FCC), effective October 16, 2013. However, businesses cannot escape liability simply by obtaining prior express consent, as more businesses are being forced into multi-million dollar settlements for exceeding the scope of consent granted by their mobile customers. This Article examines recent trends in how the FCC and the courts are delineating the contours of consent for mobile text messaging under the TCPA and provides ways businesses can engage with mobile customers without running afoul of the TCPA.

---

[*] Misa K. Bretschneider, University of Washington School of Law, J.D., with honors, 2014. Thank you to William Covington for his invaluable guidance and support, and Barry E. Bretschneider for his generous feedback.

TABLE OF CONTENTS

INTRODUCTION

2014 is shaping up to be an explosive year in Telephone Consumer Protection Act (TCPA) mobile text messaging litigation. Recently, the Buffalo Bills NFL team approved a $3 million settlement for sending *three* too many text messages to the team's mobile subscribers over a two-week period in violation of the TCPA.[1] The takeaway message is clear: businesses and their counsel need to be vigilant about TCPA compliance and ensure that all mobile text communications fall within the scope of consent provided by the customer.[2] However, the available guidance is far from clear, given that the TCPA is silent as to what forms of mobile communications are permissible.[3] For instance, if

---

[1] *Don't Text & Cheer: Fan Sues Buffalo Bills for $3 Million*, U.S. CHAMBER OF COMMERCE BLOG (May 12, 2014, 11:04 am), https://www.uschamber.com/blog/don-t-text-cheer-fan-sues-buffalo-bills-3-million.

[2] While the TCPA is arguably the most important federal law applicable to mobile marketing, it is important to note the existence of other relevant consumer protection rules beyond the scope of this Article, such as the Federal Trade Commission's analogous Telemarketing Sales Rule (TSR). *See generally* William B. Baker, *The Complications of Doing Mobile Marketing Legally*, 17 NO. 8 J. INTERNET L. 13 (2014).

[3] *See, e.g.*, In the Matter of GroupMe, Inc./ Skype Commc'ns Petition for

a customer consents to participating in a text-based social network, can the network then send the customer an administrative text message confirming the customer's interest without violating the TCPA?[4]

In recent years, the FCC and the courts are increasingly determining the scope of consent required from the context of a given mobile transaction in light of reasonable consumer expectations and industry norms.[5] While this shift towards a more common sense approach is effectively expanding the scope of consent for mobile communications, businesses and their counsel must continue to closely monitor FCC declaratory rulings and court decisions to properly assess compliance risks. This Article examines emerging trends in delineating the scope of consent for mobile text messages under the TCPA. Part I describes the rationale and relevant rules governing consent under the TCPA. Part II then analyzes two recent FCC declaratory rulings and three recent court decisions. Finally, Part III focuses on three common instances where unwary businesses can exceed the scope of consent granted by their mobile customers, and provides recommendations for minimizing such risks.

I. THE TELEPHONE CONSUMER PROTECTION ACT

In 1991, Congress enacted the TCPA to protect consumers from the growing numbers of telemarketing calls and faxes that

---

Expedited Declaratory Ruling Rules & Regulations Implementing the Tel. Consumer Prot. Act of 1991, 59 Communications Reg. (P & F) 1554 (F.C.C. Mar. 27, 2014) (finding that the TCPA is ambiguous as to how a consumer's consent should be obtained); *see also* Michael O'Rielly, *TCPA: It's Time to Provide Clarity*, OFFICIAL FCC BLOG (Mar. 25, 2014), http://www.fcc.gov/blog/tcpa-it-time-provide-clarity ("[TCPA's] lack of clarity [is] evidenced by an increasing number of TCPA-related law suits and a growing backlog of petitions pending at the FCC.").

[4] Although the FCC determined in a March 27, 2014 declaratory ruling that such texts are proper under the TCPA, other consent issues remain, such as whether consent is extinguished for reassigned phone numbers.

[5] *See, e.g.*, Aderhold v. Car2go N.A., LLC, No. C12–489RAJ, 2014 WL 794802, at *8 (W.D. Wash. Feb. 27, 2014) ("Many courts . . . have nonetheless found consent to send text messages based on the context of the transaction in which a consumer provides her cellular number.").

one TCPA sponsor deemed the "scourge of modern civilization."[6] However, rather than prohibit all forms of commercial communications, Congress "aimed to strike a balance between protecting consumers from unwanted communications and enabling legitimate businesses to reach out to consumers that wish to be contacted."[7] As a result, both the FCC and the courts grant considerable weight to legislative intent when analyzing a TCPA case.[8]

In relevant part, the TCPA prohibits businesses from making any mobile "call" without the "prior express consent" of the customer with limited exceptions, such as calls made for emergency purposes.[9] The prohibition of "calls" extends to text messages, such as those sent via Short Message Service (SMS), as well as voice calls.[10] While the TCPA does not define what constitutes "prior express consent," Congress delegated authority to the FCC to establish rules and regulations to implement the TCPA, whereby the FCC's interpretations of TCPA are controlling unless invalidated by a court of appeals.[11] Accordingly, federal district courts consistently refer to the FCC's interpretation of the TCPA when deciding TCPA cases.[12]

---

[6] *See, e.g.*, *Telemarketing and Robocalls*, FCC ENCYCLOPEDIA, http://www.fcc.gov/encyclopedia/telemarketing (last visited Aug. 22, 2014).

[7] O'Rielly, *supra* note 3.

[8] *See, e.g.*, *Aderhold*, 2014 WL 794802, at *4 ("[T]hose courts, and others, have been guided by the legislative purposes of the TCPA."); *see also* In the Matter of GroupMe, Inc./ Skype Commc'ns Petition for Expedited Declaratory Ruling Rules & Regulations Implementing the Tel. Consumer Prot. Act of 1991, 59 Communications Reg. (P & F) 1554 (F.C.C. Mar. 27, 2014) [hereinafter *GroupMe*] (exercising discretion to interpret the consent requirement by looking to the legislative goals underlying the TCPA).

[9] 47 U.S.C. § 227(b)(1)(B).

[10] *See, e.g.*, *Satterfield v. Simon & Schuster, Inc.*, 569 F.3d 946, 954 (9th Cir. 2009) (affording deference to FCC's interpretation of the TCPA that a text message is a "call" within the TCPA).

[11] *See* 28 U.S.C. § 2342 (the "Hobbs Act"); *see also* Baird v. Sabre Inc., No. CV 13-CV–999 SVW, 2014 U.S. Dist. LEXIS 11246, at *5 (C.D. Cal. Jan. 28, 2014) (stating that under the Hobbs Act, the federal courts of appeals have exclusive jurisdiction to determine the validity of final FCC orders).

[12] However, it is important to note that FCC Declaratory Rulings are not binding on courts, and thus may serve only as a source of persuasion. *See, e.g.*, Dish Network, L.L.C. v. FCC, 552 Fed. Appx. 1 (D.C. Cir. 2014).

While non-telemarketing messages, such as purely informational and non-commercial messages, require "prior express consent," heightened TCPA consent rules effective October 16, 2013,[13] require businesses to obtain a consumer's "prior express *written* consent" before sending a telemarketing message.[14] The writing requirement can be met through any legally recognized electronic or digital form, such as one that conforms to E-SIGN.[15] Notably, the inclusion of the writing requirement adds an extra hurdle for businesses seeking permissible consent: whereas businesses can obtain "prior express consent" either explicitly or implicitly through any reasonable method,[16] they must explicitly obtain "prior express written consent" by obtaining clear written consent authorizing the delivery of specified telemarketing messages.[17] Thus, a business can unwittingly exceed the scope of consent if, despite obtaining prior express consent, it sends a text message to a customer that does not fully comply with the terms provided for in the written consent agreement.

As aforementioned, the vast majority of TCPA claims focus on non-consent cases. The reason for the popularity of such cases is that prior express consent is an affirmative defense and businesses

---

[13] The revised TCPA Rules provide for other revisions, such as elimination of the "established business relationship" exemption for certain telemarketing calls. Other notable changes provide that a seller cannot require the consumer to consent to receive an automatic telephone dialing system call as a condition for a purchase.

[14] Federal Communications Commission, "Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991," Report and Order, FCC 12-21 at ¶ 15 (Feb. 15, 2012); 47 CFR § 64.1200(f)(8) ("The term *prior express written consent* means an agreement, in writing, bearing the signature of the person called that clearly authorizes the seller to deliver or cause to be delivered to the person called advertisements or telemarketing messages using an automatic telephone dialing system or an artificial or prerecorded voice, and the telephone number to which the signatory authorizes such advertisements or telemarketing messages to be delivered.").

[15] *See generally* 29 IAN C. BALLON, E-COMMERCE AND INTERNET LAW: TREATISE WITH FORMS (2nd ed. 2014).

[16] *See GroupMe*, *supra* note 8, at 3 ("[N]either the Commission's implementing rules nor its orders require any specific method by which a caller must obtain such prior express consent for non-telemarketing calls to wireless phones.").

bear the burden of demonstrating that they obtained proper prior express written consent from the customers.[18] Accordingly, in defending against a TCPA non-consent claim, a business must either show that the mobile marketing text message fell within the scope of consent provided or was altogether exempted from the TCPA.

II. DELINEATING THE SCOPE OF CONSENT

In light of Congress's intent that the TCPA "not be a barrier to normal, expected, and desired business communications,"[19] both the FCC and the courts have increasingly adopted a more common sense approach to evaluating consent for text message communications. While a common sense approach effectively broadens the scope of consent, defining the precise contours of consent is anything but common sense. This Part will provide some clarity by analyzing two FCC declaratory rulings and three court cases addressing prior express consent for mobile text messaging under the TCPA.

A. 2014 FCC Rulings

On March 27, 2014 the FCC released two declaratory rulings concerning GroupMe, Inc. (GroupMe) and Cargo Airline Association (CAA) that provided insight into the FCC's viewpoint on expanding consent to intermediaries and exempting certain text messages from the TCPA, respectively. While the rulings contain important caveats and have limited application given the fact-intensive holdings, both rulings are favorable to businesses and imply a trend towards a less strict and more practical interpretation

---

[18] *See* Olney v. Job.com, Inc., 1:12-CV-01724-LJO, 2014 WL 1747674, at *3 (E.D. Cal. May 1, 2014) (citing Pinkard v. Wal–Mart Stores, Inc., No. 3:12–CV–2902–CLS, 2012 WL 5511039, at *3 (N.D. Ala. Nov. 9, 2012)) ("Prior express consent is an affirmative defense, meaning that the defendant bears the burden of proving it.").

[19] *See, e.g.*, *GroupMe*, *supra* note 8, at 3; *see also* H.R. REP. NO. 102-317, at 17 (1991) ("The restriction . . . does not apply when the called party has provided the telephone number of such a line to the caller for use in normal business communications.").

of prior express written consent under the TCPA.

The GroupMe declaratory ruling involved a free group text messaging service that allows a customer, per GroupMe's terms and conditions, to create a group after representing that each individual added to the group has consented to be added and to receive text messages. In turn, GroupMe then sends group members up to four non-telemarketing text messages related to using and canceling GroupMe's group texting service. In relevant part, GroupMe petitioned the FCC to clarify whether these non-telemarketing text messages sent to group members, whereby consent was obtained through a group organizer intermediary, were proper under the TCPA.

In response, the FCC concluded that in this context,[20] (1) the administrative texts did not violate the TCPA because the texts constituted "normal business communications" to be expected and desired by the consenting customer, and (2) consent obtained via an intermediary was proper because such consent facilitated these normal business communications that the TCPA was not designed to prevent.[21] In acknowledging that a customer's consent "extends to a wide range of calls 'regarding' that transaction,"[22] the FCC found that when a customer voluntarily provides her number to a group organizer for participating in a GroupMe group, the GroupMe administrative texts are sufficiently related to the underlying business transaction, and thus fall within the scope of consent provided by the customer.

In its CAA ruling,[23] the FCC went a step further and altogether exempted certain free-to-the-end-user notification text messages that a package delivery company sent to customers. Although it could have based the ruling just on an intermediary consent

---

[20] The holding had the important limitation that a group organizer may only *convey* the consumer's prior express consent and that GroupMe was still liable for breaching the TCPA if the group organizer had not in fact obtained proper consent. However, this only imposed a condition and not a limitation on the scope of consent.

[21] *GroupMe*, *supra* note 8, at 4.

[22] *Id.*

[23] In the Matter of Cargo Airline Association Petition for Expedited Declaratory Ruling Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, 2014 WL 1266071 [hereinafter *CAA Order*].

theory,[24] the FCC instead exempted such text messages from the TCPA, under certain pro-consumer conditions,[25] on grounds that such text messages would protect consumer's privacy interests while improving the odds of a successful delivery. Similar to its approach in GroupMe, the FCC looked to the realities of the package delivery industry and consumer trends in concluding that alternative modes of communication would be unduly burdensome and unnecessary for package delivery companies and their customers.[26]

Despite their fact-intensive holdings, both rulings support the FCC's increasing openness to adopting a definition of consent that protects normal business communications bearing a sufficient nexus to the underlying consented transaction, even if a consumer does not individually consent to a given communication and does not give direct consent to the sender of the text. Indeed, as businesses are expanding their communications channels in response to increasing consumer expectations for more personalized brand experiences, the FCC will likely continue to expand its interpretation of consent to accommodate such evolving communications.[27] However, the FCC has also been explicit that any allowances or exemptions to consent be message-specific, and any business exceeding this scope to even the smallest degree will be liable.[28]

B. 2014 Court Rulings

In comparison to the FCC, the courts have historically been more resistant to expanding the definition of consent under the

---

[24] *Id.* at 3.

[25] *Id.* at 5 (exempting CAA's messages from the TCPA under seven conditions, including that text messages not contain any advertising component and must include opt-out procedures).

[26] *Id.* (finding that evidence of residential consumers' experience, who already receive these notifications and have not complained to the FCC, supports exempting such communications from the TCPA).

[27] *See generally* Robert Passikoff, *Brand and Marketing Trends for 2014*, FORBES (Dec. 4, 2013, 11:27 AM), http://www.forbes.com/sites/robertpassikoff/2013/12/04/brand-and-marketing-trends-for-2014/.

[28] *See, e.g.*, *CAA Order*, *supra* note 23, at 5.

TCPA. For instance, courts have differed on whether express consent can be implied from the customer's mere act of providing a cellphone number.[29] However, the emerging judicial trend is towards a more business-friendly approach that focuses on industry-specific consumer expectations and business norms. Furthermore, although the courts still privilege consumer protection in light of the TCPA's rationale, the courts are holding customers to a "reasonable consumer" standard that assumes an arguably savvy and informed customer.

For instance, in *Baird v. Sabre*, the court found that a customer, in providing her mobile telephone number to complete a flight reservation, had "voluntarily" provided her number, and thus consented to receive flight-related notification text messages from both the flight company and its third-party contractors. The customer argued that she felt compelled to provide her number in order to finalize the sale and that a reasonable consumer would "not naturally assume" that she expressly consented to be contacted at that number by a third party contractor. However, the court disagreed by adopting a reasonable airline customer standard. Specifically, the court found that a "reasonable consumer" would understand that consenting to receive a flight-related text message from the airline's contractor "fell within the scope of her prior express consent." In its holding, the court assumed that the average airline customer was a fairly well-informed customer who would understand the complex dynamics of modern advertising, even if the actual customer was not in fact so savvy.[30]

Similarly, in *Aderhold v. Car2go*, the court refused to take a narrow view of prior express consent.[31] In registering for a Car2go

---

[29] *E.g.*, Leckler v. CashCall, Inc., 554 F. Supp. 2d 1025 (N.D. Cal. 2008), *vacated*, 2008 WL 5000528 (N.D. Cal. Nov. 21, 2008) (expressing doubts about FCC's analysis granting "implied consent" that "flies in the face of Congress' intent"). *But see* Baird v. Sabre Inc., No. CV 13-CV–999 SVW, 2014 U.S. Dist. LEXIS 11246, at *6 (C.D. Cal. Jan. 28, 2014) (sympathizing with *Leckler* court's doubts regarding FCC's interpretation but nevertheless deferring to FCC's definition of consent).

[30] Baird v. Sabre Inc., No. CV 13-CV–999 SVW, 2014 U.S. Dist. LEXIS 11246, at *6 (C.D. Cal. Jan. 28, 2014).

[31] Aderhold v. Car2go N.A., LLC, No. C12–489RAJ, 2014 WL 794802, at *8 (W.D. Wash. Feb. 27, 2014).

membership, the customer entered his mobile contact number and affirmatively clicked three boxes to accept Car2go's policies. Car2go's policies, which were contained in three separate documents, specified that Car2go would later "confirm acceptance of the application."[32] Although Car2go's policies did not explicitly state that it would send the customer a text message containing activation instructions, the court found that "no reasonable person in his shoes could have doubted that Car2go would contact him in some manner."[33] Accordingly, the court found that the message contacting the customer was "closely related" to the underlying membership activation agreement since its purpose was to finalize membership, and thus fell within the scope of the customer's consent. Moreover, the court concluded that even if Car2go made no disclosures regarding how it would use the customer's cellphone number, it "defie[d] logic to contend that [the customer] did not consent to be contacted regarding his membership application."[34]

In contrast, in *Sherman v. Yahoo!*, the court denied Yahoo!'s motion for summary judgment, finding that it was an issue of fact whether a single notification text message to a consumer as part of Yahoo!'s Instant Messenger service was sent without the consumer's consent because neither Yahoo! nor the third party who facilitated the text message obtained the consumer's prior consent.[35] Unlike the customers in *Baird* and *Car2go*, who received a single text message directly related to a consumer-initiated transaction, the customer in *Sherman* did not initiate the service, and thus it was not clear that they did not expect or desire to receive a message from Yahoo!.[36] The *Sherman* court affirmed that "[c]ontext is indisputably relevant to determining whether a particular [message] is actionable" and concluded that the context underlying the transaction did not explicitly or impliedly support a finding of consent.[37]

---

[32] *Id.* at 5.
[33] *Id.* at 6.
[34] *Id.*
[35] Sherman v. Yahoo! Inc., 2014 WL 369384, *1 (S.D. Cal. 2014).
[36] *Id.* at 5.
[37] *Id.* at 6.

In all three cases, the courts adopted a fact-intensive inquiry rooted in common sense that aimed to balance consumer privacy and normal business communications. While the cases presented different fact scenarios, the decisions hinged primarily on three things: (1) the precise language contained in the disclosure documents, (2) the purpose and timing of the text message, and (3) the relationship between the sender and initiator of the text message. Part III of this Article discusses ways that businesses and their counsel can mitigate TCPA risk regarding text message communications, in light of the aforementioned factors.

III. MOBILE COMMUNICATIONS OUTSIDE THE SCOPE OF CONSENT

Despite the recent FCC and court rulings providing a broader and more practical reading of consent, businesses and their counsel must remain vigilant to prevent erroneously exceeding prior express consent under the TCPA.[38] This Part highlights three common instances where businesses can exceed the scope of a customer's prior express consent under the TCPA and recommends ways to mitigate such risk.[39]

---

[38] It is important to note that aside from limited exceptions, the TCPA does not preempt state laws that impose more restrictive requirements. *See, e.g*., Patriotic Veterans, Inc. v. State of Indiana, No. 11-3265, 2013 WL 6114836 (7th Cir. Nov. 21, 2013) (finding that Congress did not intend to create preemption when it enacted the TCPA). Indeed, Connecticut recently enacted a mini-TCPA state statute that mirrors the TCPA but provides for statutory damages of up to $20,000 per violation. *See, e.g.*, *Strengthened Connecticut Law Supplements TCPA*, KILPATRICK TOWNSEND (June 3, 2014), http://www.kilpatricktownsend.com/en/Knowledge_Center/Alerts_and_Podcasts/Legal_Alerts/2014/06/Strengthened_Connecticut_Law_Supplements_TCPA.aspx. Thus, although beyond the scope of this Article, it is critical to closely watch both state and federal developments in the area of mobile marketing text messages.

[39] While most of the cited cases directly concern text message communications, a few relate to mobile phone calls, and thus inferences will be drawn by analogy. *See, e.g.*, Satterfield v. Simon & Schuster, Inc., 569 F.3d 946, 954 (9th Cir. 2009) (finding that a "voice message or a text message are not distinguishable in terms of being an invasion of privacy" under the TCPA).

A. Language in Disclosure Documents

The first way that businesses and their counsel can protect against TCPA consent claims is to ensure that their mobile text communications do not exceed, even in the slightest degree, the conditions set forth in their customer disclosures governing such communications.

The courts meticulously analyze a business's disclosure documents, such as the terms and conditions, privacy policy, and registration documents, to determine whether the given text message communication falls within the scope of these disclosures.[40] It is not necessary that the disclosures related to the text message communication be explicitly stated and neatly contained in one document. Indeed, the disclosures may be spread across multiple documents and contain a general statement, such as "the business will confirm acceptance of the application," without explicitly stating the precise mode of communication.[41]

However, should a business choose to use precise language in its disclosure documents, a court will hold the business to that precise standard. For example, a business disclosing that it will text a customer up to five text messages per week will likely be held to that exact number, and *any* text messages exceeding this number, even one, will likely be read as exceeding the scope of the customer's consent under the TCPA.[42] Accordingly, to prevent an erroneous deviation, it is best practice for businesses to use general, rather than specific, language in their disclosure documents.

---

[40] *See, e.g.*, Aderhold v. Car2go N.A., LLC, No. C12–489RAJ, 2014 WL 794802, at *5 (W.D. Wash. Feb. 27, 2014) (closely analyzing Terms and Conditions, Trip Process, and Privacy Policy documents controlling customer's membership application and subsequent participation in the trip process).

[41] *Id.* at 6.

[42] *Don't Text & Cheer: Fan Sues Buffalo Bills for $3 Million*, U.S. CHAMBER OF COMMERCE BLOG (May 12, 2014, 11:04 am), https://www.uschamber.com/blog/don-t-text-cheer-fan-sues-buffalo-bills-3-million.

B. Purpose and Timing of Text Messages

In addition, businesses and their counsel must ensure that the purpose and timing of any text message communication are consistent with the customer's consent.

First, the purpose of a text message communication may be for promotional or informational purposes, or a combination of the two. A message containing a mix of telemarketing and non-telemarketing information constitutes a "dual purpose" message. Courts closely analyze messages and will find that a message contains a promotional element if there is either a direct or implied sales offer.[43] Accordingly, if a customer only consents to receiving an informational message, the business cannot then send a promotional[44] or a dual-purpose message.[45]

On the other hand, courts are more forgiving about the content of a given informational text message, finding that the "TCPA does not require the call to be for the exact purpose for which the number was provided."[46] However, the content of the message must bear sufficient relation to the product or service for which the customer provided her number. Accordingly, businesses must ensure that any text message relates to the same or a closely connected product or service. Furthermore, as mentioned before, a heightened level of consent is required for telemarketing messages. Thus, businesses must ensure that the purpose of a text message

---

[43] Chesbro v. Best Buy Stores Inc., 697 F.3d 1230, *as amended by* 705 F.3d 913 (9th Cir. 2012) (finding that a text message warning of the expiration of rewards points, and instructing how to preserve them, was a telemarketing message).

[44] *See e.g.*, Connelly, et al., v. Hilton Grand Vacations Co., LLC, 2012 U.S. Dist. LEXIS at *11 (S.D. Cal. 2012) (holding that hotel company sending promotional texts to customers, who made hotel reservations and submitted their cell phone numbers, exceeded the scope of consent).

[45] *See, e.g.*, Chesbro v. Best Buy Stores L.P., 705 F.3d 913 (9th Cir. 2012) (finding that scope of consent was exceeded when consent was given for only informational calls, but business later sent dual-purpose call).

[46] *See, e.g.*, Olney v. Job.com, Inc., 1:12-CV-01724-LJO, 2014 WL 1747674, at *6 (E.D. Cal. May 1, 2014) (noting that educational company could send educational-related calls, finding that employment-related calls may be sufficiently related to underlying transaction, depending on the factual circumstances).

communication is compliant with both the dual TCPA standards and the customer's consent.

Second, regarding timing, businesses must be careful that they send text messages and obtain a customer's mobile number within a proper timeframe. For instance, the FCC ruled that only confirmatory messages sent within five minutes of an opt-out request will be presumed to fall within the scope of a customer's consent, and the sender bears the burden of showing any delay was in fact reasonable.[47] Furthermore, a business must ensure that it receives a customer's mobile contact information *before* the finalization of the business transaction.[48] Accordingly, the inflexible timeframe means that businesses must ensure that proper mechanisms are in place to acquire customers' mobile numbers and send mobile communications in a timely fashion.

C. Third Party Affiliates

The final way that businesses and their counsel can protect against TCPA consent claims is to ensure that all text message communications are sent by third parties closely affiliated with the business, where the content of such communication bears a sufficient relation to the service or product for which the customer provided her number.[49] Even if the consumer did not explicitly consent to receiving text messages from an affiliated entity, courts will apply a "reasonable customer" standard in determining whether a customer's consent extends to receiving messages from third-party contractors. In recent cases, courts have extended the scope of consent to third-party messages related to the transaction

---

[47] In the Matter of SoundBite Communications Petition for Expedited Declaratory Ruling Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, 27 F.C.C.R. 15391, 15391, 2012 WL 5986338.

[48] *See* Meyer v. Portfolio Recovery Associates, LLC, 696 F.3d 943 (9th Cir. 2012) (finding that procurement of cell phone number after original business transaction does not amount to proper consent under the TCPA).

[49] *See, e.g.*, Baird v. Sabre Inc., No. CV 13-CV–999 SVW, 2014 U.S. Dist. LEXIS 11246 (C.D. Cal. Jan.28, 2014) (finding that text messages sent from an airline's third part vendor concerning flight-related matters fell within the scope of consent that the customer gave to the airline).

that a reasonable customer could assume and expect to receive, but courts have not extended the scope of consent to messages sent by a completely unaffiliated company in a separate industry.[50]

Furthermore, if a third party hired by a business sends a mobile marketing text message without consent to a consumer in violation of the TCPA, the business may be held vicariously liable under federal common law agency principles.[51] Indeed, no formal agency relationship is required for liability, and a business can also be held liable through the principles of apparent authority or ratification.[52] Accordingly, businesses and their counsel must pay attention to reasonable consumer expectations and their relationships with third party senders when initiating mobile marketing text messages.

CONCLUSION

The FCC's and courts' recent adoption of a common sense analysis will allow businesses to more freely communicate with their mobile customers, so long as such communications align with reasonable consumer expectations and established business norms. However, businesses and their counsel must implement comprehensive safeguards to protect against TCPA consent claims. Because courts are split on good faith defenses,[53] it is necessary not to make any assumptions regarding consent, even if made in good faith. Accordingly, as it is likely that the FCC and the courts will continue to expand the scope of consent under the TCPA, it is a smart business practice to adapt consent and disclosure policies in a piecemeal fashion to the evolving TCPA legal landscape.

---

[50] *See Satterfield*, *supra* note 38, at 955 (concluding that text messages sent from a cellphone provider's unaffiliated publishing company concerning publishing related matters fell outside the scope of consent that consumer provided to cellphone provider).

[51] *See*, *e.g.*, In re DISH Network, LLC, 2013 WL 1934349, FCC 13-54 (May 9, 2013).

[52] *Id.*

[53] *See*, *e.g.*, Olney v. Job.com, Inc., 1:12-CV-01724-LJO, 2014 WL 1747674, at *8 (E.D. Cal. May 1, 2014) (noting that while some courts have suggested that the TCPA is a strict liability statute, other courts have allowed for a good faith exception to liability).

PRACTICE POINTERS

- Since the statute of limitations for a federal TCPA claim is four years, it is important to keep records of customer consent for at least four years.
- When in doubt, do not make any assumptions. Although the FCC's effort to clarify the TCPA through declaratory rulings is not very efficient, one option is to petition the FCC for an expedited declaratory ruling.
- The consent rules are merely a floor. Just because a form of mobile communication may be permitted under the TCPA does not prevent customers from finding such communications annoying and seeking out competitors with less invasive communication strategies.
- In the event of a TCPA consent claim, argue that the text message was within the scope of consent provided and that consent in such case would not frustrate TCPA's underlying rationale.

WASHINGTON JOURNAL OF LAW, TECHNOLOGY & ARTS
VOLUME 10, ISSUE 1 SUMMER 2014

FIXED PERSPECTIVES: THE EVOLVING CONTOURS OF THE FIXATION REQUIREMENT IN COPYRIGHT LAW

Evan Brown[*]

Cite as: 10 Wash. J.L. Tech. & Arts 17 (2014)
http://digital.lib.washington.edu/dspace-law/handle/1773.1/1388

ABSTRACT

To qualify for copyright protection under the current Copyright Act, a work must, inter alia*, be fixed in a tangible medium of expression. This requirement is easily met when a work is embodied in a historical medium of mass expression like a printed book, photograph, or audio recording. However, when an author departs from such established media of fixation, the requirement can create a more significant barrier to copyrightability. Three decades ago, digital media provided one such challenge. Today, authors and lawyers alike are pushing the conceptual boundaries of communicative media, and this has led to some controversial recent judicial decisions on fixation. This Article contextualizes and explores the implications of those decisions. It also points out some of the practical and conceptual pitfalls that lawyers and courts may encounter in similar cases as the limits of fixation are further tested.*

---

[*] Evan Brown, Class of 2014. I would like to thank Prof. Zahr Said of the University of Washington School of Law for providing essential feedback and helping me to develop my thinking on this topic. I would also like to thank the many editors with whom I worked on the *Washington Journal of Law, Technology & Arts* over the past two years, whose efforts have shaped both the journal as a whole and this small contribution to it.

TABLE OF CONTENTS

INTRODUCTION

Fixation is a key component of federal copyright law: it is what separates protectable from unprotectable original works of authorship. It is the reason why a novel utterance is not protected but a novel sound recording is. While copyright law creates intellectual property rights, the fixation requirement ensures that the intellectual property right can be tied to a physical object. To put it another way, an author's work needs an avatar to qualify for protection. The process of fixation merges "original work and tangible object . . . in order to produce subject matter copyrightable under the [Copyright Act]."[1] Only once this merger has occurred is a work properly copyrightable.

Fixation is necessary because only fixed works are at risk of misappropriation by copying. Copyright law is grounded in the incentivization of artistic *production*, not mere creativity. As a matter of policy, copyright encourages making and distributing works that can communicate expression to others far and wide. Its imposition of limited monopoly rights is interest charged on the debt we owe to the printing press. The net effect of these

[1] H.R. REP. NO. 94-1476, at 51 (1976).

requirements is familiar and fundamental to copyright law: an expression only constitutes a copyrightable work if it can be reproduced, performed, displayed, or distributed. Copyright protects things that can be copied, not things that can be imitated.

The historically dominant media of mass expression are the progenitors of the fixation requirement: printed books and periodicals, paintings, photographs, film, and musical recordings are the sort of media that copyright law has long championed. There is a practical, if not a legal, presumption that works in these media are appropriately fixed. But more difficult cases have emerged in recent years as unusual media of expression have had their day in court. These cases bring to the forefront questions about which types of works copyright law encompasses. In considering these questions, we must also consider, as a policy matter, which types of works copyright should incentivize as creators test the boundaries of authorship and expression.

I. THE FIXATION REQUIREMENT

The fixation requirement is defined in 17 U.S.C. §102(a), which applies copyright protection to "original works of authorship *fixed in any tangible medium of expression*, now known or later developed, *from which they can be perceived, reproduced, or otherwise communicated*, either directly or with the aid of a machine or device."[2] Section 101 offers further insight: "A work is 'fixed' in a tangible medium of expression when its *embodiment* . . . is *sufficiently permanent or stable* to permit it to be perceived, reproduced, or otherwise *communicated* for a period of *more than transitory duration*."[3] By combining these provisions, the

[2] 17 U.S.C. § 102(a) (2006) (emphasis added).

[3] 17 U.S.C. § 101 (emphasis added) (definition of "fixed"). The statute also requires that embodiment be in a "copy" or "phonorecord." Copies are in turn defined as "material objects, other than phonorecords, in which a work is fixed by any method now known or later developed, and from which the work can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device." *Id.* (definition of "copies"). Phonorecords, on the other hand, are restricted to "material objects in which sounds, other than those accompanying a motion picture or other audiovisual work, are fixed by any method now known or later developed, and from which the sounds can be

requirement seems reducible to four basic elements: (1) encoding of expression (2) in a physical medium (3) that can convey that expression to others (4) and can persist unaltered for some appreciable time. Notably, only the first of these elements involves creative activity by the author; the latter three are qualities of the medium in which the author encodes the expression.

The fixation requirement can be satisfied in a number of situations. The author can make the material copy before the work is ever presented to an audience.[4] The author can make the material copy *while* the work is first being presented to an audience.[5] The author can even direct another person to make the first copy.[6] In each case, the key is that the expression is preserved in some persistent communicative medium, some useable vehicle for later communication. This is what separates copyable (and thus potentially copyrightable) expression from uncopyable expression.

A. The Origins of Fixation

For most of the history of copyright law, fixation has not been an issue. It was simply an undifferentiated part of the authorship process,[7] while copyrightable subject matter was confined to rigid

---

perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device." *Id.* (definition of "phonorecords). These definitions accomplish little more than dividing acceptable media of fixation into (1) audible media and (2) all other media of expression.

[4] *See* 17 U.S.C. § 101 (definition of "fixed").

[5] *Id.* ("A work consisting of sounds, images, or both, that are being transmitted, is 'fixed' for purposes of this title if a fixation of the work is being made simultaneously with its transmission."); *see also* Baltimore Orioles, Inc. v. Major League Baseball Players Ass'n, 805 F.2d 663, 675 (7th Cir. 1986) (holding that simultaneous recording of a baseball game constitutes fixation of the players' performances).

[6] 17 U.S.C. § 101 (definition of "fixed," noting that fixation may be accomplished "by or under the authority of the author"); *see also* H. R. REP. NO. 94-1476, at 51–2 (exploring fixation in the context of a directed broadcast).

[7] It was, in fact, Congress's expansion of the concept of authorship that necessitated the fixation requirement. In refusing to confine authorship to certain categories of works, Congress chose to broaden the concept of a work. *See* H. R. REP. NO. 94-1476, at 51–2. The fundamental qualities of the concept of a work, it seems, were human agency, expression, and fixation. *Id.*

categories rather than defined by flexible concepts and qualities. The first U.S. Copyright Act, enacted in 1790, applied quite specifically to maps, charts, and books only.[8] Congress extended protection to musical compositions in 1831.[9] In 1909, the list of categories was greatly expanded to include periodicals, prepared speeches, dramatic compositions, drawings, prints, photographs, and "works of art."[10]

Only when this periodic expansion seemed destined to continue ad infinitum did Congress attempt to craft a more flexible solution. This solution was to make the subject matter requirement dependent on the qualities of its creation rather than on the categorization of expressive products.[11] While Congress did not abandon entirely the attempt to categorize works of authorship—indeed, it expanded those categories yet again[12]—it chose not to confine copyright protection to its enumerated categories.[13] Suddenly, fixation mattered as a concept.

The historical media of authorship all required fixation, and in an important way they defined the concept. They were media, but they were a particular *kind* of media. They were media that involved an encoding of expression in a durable physical form. They could be distributed, experienced, kept, and reused. Most importantly, they could be copied. Their value was intertwined with their vulnerability. Copyright law incentivized their creation by addressing the vulnerability while preserving the value.

But as technology advanced and the panoply of expressive media expanded, a more fluid concept was required to keep pace. Recognizing that "[a]uthors are continually finding new ways of expressing themselves, [and] it is impossible to foresee the forms that these new expressive methods will take," Congress added the fixation requirement as a sort of flexible gatekeeper for the

---

[8] Copyright Act of 1790, 1 Stat. 124 § 1; *see also* H. R. REP. NO. 94-1476, at 51–2.

[9] Copyright Act of 1831, 4 Stat. 436 chap. 16.

[10] Copyright Act of 1909, Public Law 60-349 § 5.

[11] *See* H. R. REP. NO. 94-1476, at 51–2.

[12] *See* 17 U.S.C. § 102(a)(1–8).

[13] 17 U.S.C. § 102(a) ("Works of authorship *include* the following categories . . . .") (emphasis added); *see also* H. R. REP. NO. 94-1476, at 51–2.

protection of new media.[14] Yet, despite the flexibility afforded by trading fixed categories for their defining conceptual quality, new technology still managed to create confusion over copyrightability as the digital revolution began.

B. Fixation in the Digital Age

Digital works presented two different problems for fixation, one of technological literacy and one of categorical characterization. Digital works appeared, at least to the untrained user, to be intangible by nature. Since copyrightability turned on whether an expressive medium was also a tangible medium, courts were called on to determine tangibility. At the same time, the emergence of interactive digital works—specifically, video games in their industrial infancy—challenged courts to assess what characteristics must be unchangeable to qualify as a fixed work.

1. The Tangibility of Digital Works

The question of tangibility was the simplest for the courts to answer. Despite a general lack of institutional competency with regard to new technologies, courts were able to arrive at a workable solution by analogy. At least one early court that considered the issue held that programs could not be fixed in computer memory, likening such memory to building plans.[15] Yet the legislative history behind the Copyright Act showed that the development of computer programs and other digital works was a key impetus for the shift from categorical protection to the flexible fixation requirement.[16] Taking this into account, courts began to look at the question more practically, and a consensus emerged that most memory media were adequate media of fixation.[17] The

---

[14] *See* H. R. REP. NO. 94-1476, at 51.

[15] Data Cash Sys., Inc. v. JS&A Grp., Inc., 480 F. Supp. 1063, 1066 n.4 (N.D. Ill. 1979) (concluding in dictum that a computer program could not be fixed in memory because the memory was analogous to a playback device, not a tangible medium of expression).

[16] H. R. REP. NO. 94-1476, at 52.

[17] *E.g.*, Tandy Corp. v. Pers. Micro Computers, Inc., 524 F. Supp. 171, 173

key to these decisions was that humans could encode computer programs—which the courts agreed were works of authorship—onto the memory for later playback. While computer memory operated in some sense as a playback device, it was the fact that it could store a work for playback that made it an acceptable medium of fixation. That made memory more similar to the historical media of fixation—the media of mass publication—than to a mere playback device.

2. Interactivity and Fixation

Interactivity proved somewhat more difficult, though courts again ended up in accord on the issue. In *Williams Electronics, Inc. v. Artic Int'l, Inc.*, the Third Circuit considered whether an inherently changeable work could be fixed.[18] The plaintiff in that case, the producer of the early video game *Defender*, sued a copycat producer for effectively replicating the game. *Defender* had two modes: the "play mode" and the "attract mode." The latter consisted of a rotating series of set animations and sounds showing examples of what the game was like when played. The court had little difficulty concluding that this mode was fixed for purposes of copyright protection; while the presentations were generated anew from computer memory each time, they followed set patterns and therefore were always the same expression.[19] The game code and art and music assets were the sort of "machine or device" contemplated by the § 101 fixation definition.

The "play mode" at issue in *Williams* was more problematic because the actual order and arrangement of the audiovisual presentation depended on user input. When a user played the game, the arrangement of the art assets and the timing of animations and

(N.D. Cal. 1981); Stern Electronics, Inc. v. Kaufman, 669 F.2d 852, 855 n.4 (2d Cir. 1982); Williams Electronics, Inc. v. Artic Int'l, Inc., 685 F.2d 870, 874 (3d Cir. 1982).

[18] 685 F.2d at 870.

[19] *Id.* at 874 (emphasis added); *accord Stern*, 669 F.2d at 856 ("[M]any aspects of the sights and the sequence of their appearance remain constant during each play of the game. . . . The repetitive sequence of a substantial portion of the sights and sounds of the game qualifies for copyright protection as an audiovisual work.").

sound playback would change according to player's decisions and reactions. The actual course of the presentation was not fixed in the colloquial sense. Yet the court still held that the game satisfied the fixation requirement, since the player was interacting with copyrighted art and sound in set patterns determined by copyrighted instructions:

> Although there is player interaction with the machine during the play mode which causes the audiovisual presentation to change in some respects from one game to the next in response to the player's varying participation, there is always *a repetitive sequence of a substantial portion* of the sights and sounds of the game, and many aspects of the display remain constant from game to game regardless of how the player operates the controls.[20]

Essentially, the court held that the player's "changes" were only to the manner of experiencing otherwise properly copyrighted elements. The game memory, code, and kit constituted a "device" that aided the player in experiencing these fixed elements. So long as the player could recreate the exact same inputs and timing (which was nearly impossible), the same patterns would occur. Even if exact reproduction did not occur, a "substantial portion" of the presentation remained the same. The game was therefore copyrightable, and the defendant was liable for copying it.

This same principle arose from other leading cases examining the issue, and quickly became a widespread rule.[21] Fixation was, generally speaking, no longer a barrier to the development of digital works and the massive industries they spawned. The new, flexible fixation requirement had passed its first big test. But that test was not to be its last.

II. EMERGING BOUNDARIES TO MEDIA OF FIXATION

In recent years, a different sort of threat to our understanding of

---

[20] *Williams*, 685 F.2d at 874.

[21] *See Stern*, 669 F.2d 852; Midway Mfg. Co. v. Artic Int'l, Inc., 547 F. Supp. 999, 1008 (N.D. Ill. 1982).

fixation has arisen. This threat is not technological, but conceptual. Two cases—one involving conceptual artistry and the other involving creative lawyering—have brought the fixation requirement back into the limelight. This nascent line of case law began with the controversial 2011 case *Kelley v. Chicago Park District*[22] and was taken up later that year in the much less heralded case *Kim Seng Co. v. J & A Importers*.[23] In *Kelley*, the U.S. Court of Appeals for the Seventh Circuit provided controversial but nuanced reasoning distinguishing media of fixation from media inherently ill-suited to fixation. In *Kim Seng*, a California district court then took that reasoning and extended it in an apparent attempt to simplify and apply it to qualitatively similar media. While it is unclear precisely what conclusions should be drawn from this emerging line of cases, or even whether the line will be built upon further, the cases mark a significant turn in fixation jurisprudence toward circumscribing media of fixation according to qualitative characteristics of those media.

A. Kelley v. Chicago Park District

The beginnings of the new bounding of fixation began in *Kelley*.[24] In that case, the Seventh Circuit considered whether a "living art" piece comprising arrangements of planted wildflowers was sufficiently fixed to allow for copyright protection. The artist, Chapman Kelley, was a well-known Texas painter and landscape artist who conceived of the arrangement as a public work of conceptual art. He installed it in 1984 in Chicago's Grant Park and maintained it for years afterward. However, the wildflowers became overgrown and the Chicago Park District heavily modified the arrangement, reducing its size and altering its geometry. Kelley opposed the changes and ultimately sued the Park District under the new Visual Artists Rights Act (VARA). VARA, which injects into the Copyright Act limited aspects of the moral rights (*droit moral*) that underlie much of European copyright law,[25] gives an

---

[22] 635 F.3d 290 (7th Cir. 2011).
[23] 810 F. Supp. 2d 1046, 1051 (C.D. Cal. 2011).
[24] *See* 635 F.3d 290.
[25] VARA, codified at 17 U.S.C. §106A, implements a limited moral rights

artist the right to prevent modification of particular kinds of visual art, including sculptures. Kelley claimed that his "Wildflower Works" was a sculptural work, and thus subject to VARA. But to qualify as a sculpture, the work had to meet the general requirements for copyright protection as well.

Fixation proved the primary hurdle to copyright protection of the work.[26] Wildflowers were an unusual medium, one that needed continuous maintenance to achieve any real semblance of permanence. Kelley himself had described the concept for the piece as involving the "management" of living elements.[27] This management was apparently important to the conceptual expression Kelley intended. Unfortunately, it was also fatal to copyrightability, as it challenged the boundaries of permanence and made the source of authorship unclear.

The court found the concept of fixation to be fundamentally incompatible with the qualities of plant arrangements. "A garden's constituent elements are alive and inherently changeable, not fixed. . . . [I]ts appearance is too inherently variable to supply a baseline for determining questions of copyright creation and infringement."[28] Essentially, the court found that, because plants are constantly growing, there is no point at which they can give rise to more than temporary, uncopyable images. The issue was with the very essence of the medium:

> Seeds and plants in a garden are naturally in a state of perpetual change; they germinate, grow, bloom, become dormant, and eventually die. This life cycle moves gradually, over days, weeks, and season to season . . . . The essence of a garden is its vitality, not its fixedness. It may endure from season to

---

regime for well-known works of visual at in the United States. *Kelley*, 635 F.3d at 297. In 1988, the United States signed the Berne Convention for the Protection of Literary and Artistic Works, but in several respects the country subsequently failed to comply with the treaty provisions. One such provision was protection of artists' moral rights, protected by Article 6bis. Congress enacted VARA to bring U.S. copyright law into compliance.

[26] *Kelley*, 635 F.3d at 303.

[27] *Id.*

[28] *Id.* at 304–05.

season, but its nature is one of dynamic change.[29]

The court could find no point at which the plants could be considered appropriately fixed, as they were always changing. Something *vital*, something living, could not be fixed—the essence of living is growth and mortality, not permanence.

Moreover, the court did not believe that a human could actually author a garden. The court described a garden as something a human could initiate and maintain, but not something that a human could actually create. The creative forces behind the wildflowers were not Kelley's intellect and expressive act; they were the forces of nature, acting as they always do. "Most of what we see and experience in a garden—the colors, shapes, textures, and scents of the plants—originates in nature, not in the mind of the gardener."[30] Because human expression is not what gives rise to the visual elements of the work, it is not an expressive work and is therefore not subject to copyright protection.

Notably, the court did not disagree with Kelley about the expressive potential of wildflower arrangements. Instead, the conceptual rift between them was over whether that expression came via a medium, from artist to viewer, or directly from nature to viewer (with the "artist" confined at best to a curatorial role). The court juxtaposed planted gardens with landscape designs. Such designs, it noted, are copyrightable because they make the artist's expression reproducible.[31] A plant can grow on its own, but a drawn design cannot.

The court implied that non-static expressive media can exist, but they must be sufficiently static to allow for reproduction and transmission of the author's expression.[32] The court noted, for example, that Alexander Calder's continuously moving mobiles, animated by wind and other natural forces, were sufficiently fixed because the individual functional elements of the mobiles were "obviously fixed and stable."[33] Similarly, a Jeff Koons wire-frame

---

[29] *Id.* at 305.
[30] *Id.* at 304.
[31] *Id.* at 304–05.
[32] *Id.* at 305.
[33] *Id.* This example calls to mind the video game elements in *Williams*, individually fixed and functionally constrained by a set of rules authored by a

sculpture covered in living flowers was deemed likely copyrightable, as the frame should be enough to fix the expression.[34] The operative question in the Seventh Circuit's view is whether the work is "quintessentially a garden" (i.e., an "expression" of natural forces) or a work of art (i.e., a reproducible form of the *author's* expression).[35] Put another way, the court was concerned with whether nature or a human author produced the aesthetic elements of the work.

Wild plants, according to the *Kelley* decision, could not be directed by a human author, and therefore they could not serve as a medium of fixation. The court made it clear that its decision was categorical and essential. It deemed "vitality"—and, by implication, its less popular conceptual companion, mortality—the operative quality of the medium.[36] A proper medium of fixation, like the historical media of mass communication, would instead be characterized by "fixedness."[37] That is not to say that plants could not form a component of a copyrightable work, but such a work would have to be sufficiently fixed in another medium. This reasoning seemed to put a new gloss on Congress's intentionally open-ended language, effectively limiting fixation to media (old and new) that were *in essence* neither unpredictably protean nor inescapably progressive.

B. Kim Seng Co. v. J & A Importers

What was not clear in the wake of the *Kelley* ruling was whether courts might extend the holding to apply to other sorts of

---

human creator. *See* Williams Electronics, Inc. v. Artic Int'l, Inc., 685 F.2d 870, 874 (3d Cir. 1982).

[34] It is logical to believe that a court would find only the non-living elements of the latter work copyrightable, although the court here expressly declined to offer its opinion on the issue. *Kelley*, 635 F.3d at 305–06.

[35] *Id.* at 306.

[36] *Id.* at 305.

[37] *Id.* The court thereby produced an odd sort of teleology of fixation: a unfixable seed becomes an unfixable tree, but in death (or severance) it becomes fixable wood—once dead, material that in life could not constitute a copyrightable work may be formed into any manner of sculptures, paintings, photographs, or books.

inherently non-static media. The Seventh Circuit focused so intently on the living essence of plants that its holding could rather easily be limited to planted gardens alone.[38] But at least one court has taken the bait and extended the *Kelley* holding to all inherently perishable media.

In *Kim Seng Co. v. J & A Importers*, the U.S. District Court for the Central District of California had to decide whether an arrangement of food was copyrightable as a matter of law.[39] The plaintiff, a maker of Vietnamese rice sticks, had asked its employee to arrange its rice sticks with some other traditional Vietnamese foods in a bowl in a traditional manner. An outside photographer then photographed the bowl, and the company used the picture on its packaging. Because it was unclear whether the company owned the copyright to the photograph, it claimed that the underlying arrangement was itself copyrighted, with the photograph constituting only a derivative work.

The defendant moved for summary judgment on grounds that perishable food, like the living plants discussed by the Seventh Circuit in *Kelley*, was an inherently inadequate medium of fixation. The court extended *Kelley*, but in the process simplified its holding as well:

> Like a garden, which is "inherently changeable," a bowl of perishable food will, by its terms, ultimately perish. Indeed, if the fact that the Wildflower Works garden reviving itself each year was not sufficient to establish its fixed nature, a bowl of food which, once it spoils is gone forever, cannot be considered "fixed" for the purposes of § 101.[40]

The court keyed in on the stability requirement mentioned in *Kelley*, seemingly holding that any physical form that deteriorates

---

[38] Indeed, the court seemed to stop just short of limiting its holding in this very way by favorably discussing the Koons wire-frame work. *Kelley*, 635 F.3d at 305–06.

[39] 810 F. Supp. 2d 1046, 1051 (C.D. Cal. 2011) (considering plaintiff's motion for summary judgment).

[40] *Kim Seng*, 810 F. Supp. 2d at 1054.

cannot be used to fix expression for copyright purposes. Where the *Kelley* court expressly declined to hold that physical impermanence necessarily conflicted with the "sufficient permanence" required by §101—indeed, it noted that "no medium of expression lasts forever"[41]—the *Kim Seng* court found perishability dispositive of the fixation issue.

This extension was not made blindly. The court explained that "the purposes underlying the fixation requirement—to 'ease[] problems of proof of creation and infringement'—apply with equal force to a garden and a bowl of perishable food."[42] The district court, situated in the Ninth Circuit, was under no obligation to follow *Kelley*; it looked to it only as persuasive authority. And unlike the Seventh Circuit, the district court looked past issues of authorship and agency in favor of the evidentiary value of the fixation requirement. In effect, the court held that because food could not remain stable long enough to be offered as evidence in the event of an infringement claim, it could not serve as a medium of fixed expression.

By this logic, "sufficient permanence" necessarily entails sufficient stability to retain form and structure until the time of any likely trial. While the court stated quite clearly that food was inherently unfixable because it will "ultimately perish," it could not have meant that *any* physical form subject to eventual deterioration cannot serve as a medium of fixation. Such a holding would render historical media, e.g. photographs and paintings, uncopyrightable because paint and ink will fade and discolor with exposure to the elements.[43] This would also be true of sound recordings made on audio tape, which degrade over time,[44] and might even extend to electronic memory media, which degrade

---

[41] *Kelley*, 635 F.3d at 305.

[42] *Kim Seng*, 810 F. Supp. 2d at 1054.

[43] *See, e.g.*, *Preservation: Photographs*, NATIONAL ARCHIVES, http://www.archives.gov/preservation/formats/photographs.html (last visited Mar. 22, 2014). Yet the *Kim Seng* court even noted that a photograph is "obviously" an appropriate medium of fixation. *Kim Seng*, 810 F. Supp. 2d at 1054 n.8.

[44] *See generally* Richard L. Hess, *Tape Degradation Factors and Challenges in Predicting Tape Life*, 34 ASS'N FOR RECORDED SOUND COLLECTIONS 240, 244–67 (2008).

steadily with use.[45] In fact, if one takes a long enough view, no physical form is truly immune from deterioration. Thus, the key to understanding *Kim Seng* lies in its mention of evidentiary necessity, not its discussion of perishability.

If evidentiary value is at issue, it would seem that the primary requirement for fixation would be that a medium be at least *capable* of maintaining communicative permanence for the term of copyright protection. Yet this finds surprisingly little support. The *Kim Seng* court cited to the treatise *Patry on Copyright* for the proposition that evidentiary necessity supported the fixation requirement.[46] That treatise, in turn, cited to Douglas Lichtman's 2003 article *Copyright as a Rule of Evidence*.[47] But Lichtman explained in that article that

> the modern requirement excludes only those cases where there never was any physical evidence of the claimed expression; it does not exclude cases where there was evidence at some point in time, but that evidence was later lost or destroyed. Stated another way, federal law requires that fixations survive for a period of "more than transitory duration," but it does not require that fixations survive, say, until the moment of litigation.[48]

Oddly, *Kim Seng* seems to stand for exactly the opposite proposition yet indirectly cites to the article for support. Because of this, it is unclear where exactly courts looking to follow *Kim Seng*, or at least trying to interpret *Kelley* in the same way, should draw the line. If fixation requires something less than stability for the term of copyright but something more than the rapid degradation that characterizes perishable food, just how stable does a communicative medium need to be to qualify as a medium of

---

[45] *Tech Guide: Storage Media Lifespans*, ZDNET (Oct. 14, 2002), http://www.zdnet.com/tech-guide-storage-media-lifespans-1120269043.

[46] *Kim Seng*, 810 F. Supp. 2d at 1054 (citing to 2 *Patry on Copyright* § 3:22).

[47] Douglas Lichtman, *Copyright As A Rule of Evidence*, 52 DUKE L.J. 683, 732 (2003).

[48] *Id.*

fixation?

C. A Look Toward the Future

It remains to be seen whether other courts will follow the trail paved by *Kim Seng* and extend the notion raised in *Kelley* that authors simply cannot fix works in certain media. The intuitive allure of the idea is clear in both cases: how can you "fix" something that can change? But, as the *Kelley* court recognized, everything can and does change over time. Of course, categorical restrictions on media are heuristically useful as well; there is no need to determine whether a particular arrangement of plants or food is sufficiently permanent if no plants or food can be. But is this emerging approach really in line with congressional intent? And, as a policy matter, does it impose problematic restrictions?

As discussed above, Congress intended to create a flexible requirement that could adapt to new technologies and art forms. The video game cases represented an effort by courts to accommodate this intent. But categorical rejection of certain media could potentially upend that accommodation.

One issue that may be on the horizon involves a concept that computer scientists call "emergent behavior." The concept encompasses unforeseen effects of designed programs and systems. More complex systems more frequently exhibit emergent behaviors.[49] Artificial intelligence programs, extraordinarily complex and difficult to predict with certainty, often exhibit these types of behaviors.[50] In fact, emergent behaviors may well be a key to producing artificial intelligence.[51] A human can program an artificial intelligence, and that program would seem to be copyrightable as a form of software. But if that software is subject

---

[49] *See generally* Gerald E. Marsh, *The Demystification of Emergent Behavior* (2009), *available at* http://arxiv.org/abs/0907.1117.

[50] Pattie Maes, *Behavior-Based Artificial Intelligence*, *in* PROCEEDINGS OF THE FIFTEENTH ANNUAL CONFERENCE OF THE COGNITIVE SCIENCE SOCIETY, 74 (Lawrence Erlbaum Associates, 1993).

[51] *See, e.g.*, Rodney A. Brooks, *A Robot that Walks: Emergent Behaviors from a Carefully Evolved Network*, Massachusetts Institute of Technology Artificial Intelligence Laboratory, A.I. Memo 1091 (1989).

to emergent behaviors unforeseen by the author, has it really been encoded as a work? Moreover, is such a work permanent in the sense that it can resist "deterioration" from the author's original vision long enough to serve as evidence of it? Aren't these programs more akin to wildflowers in a garden than to simple programs like *Defender*?

From a policy perspective, it would seem advantageous to society to incentivize creation of these sorts of works. Copyright law in general is usually justified as incentivizing production of expressive works, often for public consumption.[52] But if the fixation requirement impedes copyright protection for work deemed important, this incentivization will be suboptimal at best. This problem may extend to artificial intelligence programs. It may also extend to conceptual art expressed through gardens or even food. If federal copyright law does not protect these sorts of works, the states may wish to step in, since the protection of unfixed works is not preempted by the Copyright Act.[53]

While these concerns may not have been on the minds of the judges who decided *Kelley* and *Kim Seng*, judges looking to those cases as persuasive authority in the future would do well to keep the implications of those decisions in mind. If they do not, and especially if the courts further narrow the boundaries around media of fixation, the courts may ironically return copyright law to the place Congress left behind in 1976: confined to known media of expression in a continuously changing world.

CONCLUSION

The courts in *Kelley*—which pitted an intransigent artist against a cash-strapped municipal agency—and *Kim Seng*—which involved dubious claims and seemingly unfair competitive practices—may well have been looking for reasons to find a lack of copyright protection. But regardless of their intentions, the courts produced a new line of intriguing case law on fixation. In an ironic twist, the concept that Congress hoped would provide

---

[52] 1 THE LAW OF COPYRIGHT § 1:3 (2010).
[53] 2 PATRY ON COPYRIGHT § 3:22 (2007).

flexibility for protection of expressive works in unknown future media may well prove a barrier to the protection, and therefore the incentivization, of such works.

Lawyers and judges alike should be aware of the turn in reasoning represented by *Kelley* and *Kim Seng*. The idea of categorical medium restrictions provides fertile soil for novel arguments and efficient rulings. But blind judicial acceptance of the potentially tantalizing approach is dangerous. The implications of the new *Kelley* line threaten to corral fixation, and therefore copyright law, within fences established by history and intuition rather than effective policy and legislative intent.

PRACTICE POINTERS

- When challenging the copyrightability of a work in a new or unusual medium, consider whether that medium is inherently self-changing or so obviously impermanent as to call into question its suitability as a medium of fixation.
- When arguing against such a fixation challenge, consider that both policy and legislative intent favor a flexible and accommodating fixation requirement.

WASHINGTON JOURNAL OF LAW, TECHNOLOGY & ARTS
VOLUME 10, ISSUE 1 SUMMER 2014

DISCOVERING THE UNDISCOVERABLE: PATENT ELIGIBILITY OF DNA AND THE FUTURE OF BIOTECHNICAL PATENT CLAIMS POST-*MYRIAD*

Alex Boguniewicz[*]

Cite as: 10 Wash. J.L. Tech. & Arts 35 (2014)
http://digital.lib.washington.edu/dspace-law/handle/1773.1/1389

ABSTRACT

In June 2013 the Supreme Court held that naturally occurring human DNA cannot be patented, but synthetically created DNA is patent-eligible. Though a major victory for patients' rights, the holding of Association for Molecular Pathology v. Myriad Genetics *appears to be the latest in a series of restrictions on patents and the human body, much to the annoyance of biotechnology companies. However, this case should not be viewed as the final word in patenting "natural phenomena." Patent claims of genetic material are still viable when the claim details a new and useful improvement on the naturally occurring product or an application of the product to a process. Furthermore, the* Myriad *Court noted that extending the natural products rule too far would be against public policy, giving litigators room to explore the contours of this rule.*

This Article examines the limits of the Supreme Court's decision and the avenues that potential patent seekers still have for making eligible patent claims on naturally occurring products and phenomena, as well as the processes for identifying such products and phenomena. It

---

[*] Alex Boguniewicz, University of Washington School of Law, Class of 2015. Thank you to Professor Toshiko Takenaka for her guidance; to Dr. Jan B. Krauß for lending his invaluable expertise; and to Matthew Fredrickson for all his help and patience.

highlights the areas where the courts are likely to take a hard stance against patent eligibility and where opportunities still exist to claim a valid patent in three areas. First, though discovery of a natural process in its naturally-occurring state is now un-patentable, the Myriad *holding signals that a variation on this natural state, no matter how slight, could make the product eligible for a patent under the "new and useful improvements" rule. Second, the "application of new processes" rule is unchanged by this case. Third, a public policy argument on the importance of protecting medical and genetic discoveries may be more relevant in light of* Myriad's *broad holding.*

TABLE OF CONTENTS

INTRODUCTION

In *Association for Molecular Pathology v. Myriad Genetics*, the Supreme Court unanimously reversed the Federal Circuit Court

of Appeals' finding that human DNA was patent-eligible.[1] The Court instead held that naturally occurring materials, even if first "discovered" by a company, do not fall within the scope of 35 U.S.C. §101 [hereinafter "§101"] and thus cannot be patented.[2] In a term that saw the Court tackle gay marriage, voting rights, and affirmative action, a case concerning patents and biotechnology did not stand out as the most vital issue. However, *Myriad* proves both a major victory in the realm of patient-subject rights and a cause of concern for the biotechnology industry.

Myriad has a complicated procedural background and is mired in difficult science. However, the Court answered in a brief opinion that discovery of genetic material, without significant changes to the natural substance, does not satisfy the "new and useful" standard under §101. While some fear that this holding will greatly restrict the incentives to engage in scientific research, *Myriad* should be seen for the opportunities it provides potential patent holders of natural products and the gaps left unaddressed. Although discovery alone may not be enough to warrant a patent, three doctrines are at a litigator's disposal in arguing for patent eligibility of genetic material. First, the reasoning of *Myriad* and its case history suggest that the courts and the United States Patent and Trademark Office will uphold claims detailing new and useful improvements, even if they are slight. Second, application of discoveries to specific processes was upheld in *Myriad*. Third, public policy arguments against over-applying the reach of the naturally occurring exemption can provide a potential fallback argument.

I. PROCEDURAL HISTORY AND THE SUPREME COURT'S DECISION

In order to understand the Supreme Court's straightforward holding in *Myriad*, one must first parse through complicated science and a heated series of decisions among the lower courts.

---

[1] 133 S. Ct. 2107, 186 L. Ed. 2d 124, 2013 WL 2631062 (June 13, 2013).
[2] *Id.*

A. Myriad's Patents

In 1994, Myriad Genetics, Inc. discovered the location and sequence of the BRCA 1 and BRCA 2 genes (pronounced brah-ka).[3] These genes and their mutations are strongly linked to an increased risk of developing breast and ovarian cancer.[4] After pinpointing the genes' locations, Myriad developed a diagnostic test to detect the presence of the BRCA mutations in an individual's DNA.[5] Myriad was issued the patents for BRCA 1 and the diagnostic test in 1997, and for BRCA 2 and the diagnostic test in 1998.[6]

Additionally, Myriad was able to extract the DNA and synthesize a strand of nucleotides referred to as complementary DNA (cDNA).[7] This synthetic DNA is produced by recreating the RNA transcription process but results in a DNA sequence distinguishable from the source genetic material.[8] As with BRCA 1 and 2 and the testing, Myriad held patents to exclusively synthesize cDNA from the BRCA genes.[9]

By 1996, the University of Pennsylvania's Genetic Diagnostic Laboratory (GDL) began providing, for a fee, BRCA 1 and 2 diagnostic tests, while other labs sent patient samples to GDL for separate BRCA tests.[10] Myriad responded with letters advising GDL researchers that it would enforce its patents, and early litigation was resolved with agreements that the labs would discontinue activity that potentially infringed on Myriad's patents.[11]

---

[3] Ass'n for Molecular Pathology v. U.S. Patent & Trademark Office, 689 F.3d 1303, 1313 (Fed. Cir. 2012). This is the appellate decision that the Supreme Court overruled. Due to its more detailed and extensive discussion of the facts and science, it will be cited for most of the case background.

[4] *Id.*

[5] *BRCA Analysis*, MYRIAD GENETICS, http://www.myriad.com/products-services/hereditary-cancers/bracanalysis/ (last visited Aug. 25, 2014).

[6] *Ass'n for Molecular Pathology*, 689 F.3d at 1313 n.5.

[7] *Id.* at 1313–14.

[8] *Id.* at 1313.

[9] *Id.* at 1309.

[10] *Id.* at 1313.

[11] *Id.* at 1315–16.

B. Road to the Supreme Court

Myriad's warning letters were merely the beginning of what would become a drawn out legal battle. After GDL's agreement, a variety of clinical laboratories, medical societies, individual researchers, health-advocacy groups, and individual breast cancer patients challenged Myriad's patents.[12] Their suit commenced in May 2009 in the District Court for the Southern District of New York.[13] The complaint alleged violations of 35 U.S.C. §101 (patentable inventions), the Copyright Clause,[14] and the First and Fourteenth Amendments.[15]

The district court quickly dismissed the constitutional claims via the avoidance doctrine, and instead focused on the scope of 35 U.S.C. §101.[16] Examining the patents for the isolated BRCA genes and cDNA, the court held that a product of nature is not patentable unless the patent holder transforms the original product to the point that the new product possesses "markedly different characteristics."[17] The court found that Myriad failed to show the BRCA genes, in isolated form, were significantly different from their natural state.[18] Even the patents for the cDNA were determined to be naturally occurring products, as they were essentially the result of a natural splicing process of pre-mRNA to mature mRNA.[19]

In regard to the "method" claims of Myriad, the court again implemented a strict reading of §101, holding that a process claim is patent-eligible only if: "(1) it is tied to a particular machine or apparatus, or (2) it transforms a particular article into a different

---

[12] Ass'n for Molecular Pathology v. U.S. Patent & Trademark Office, 702 F. Supp. 2d 181, 186–90 (S.D.N.Y. 2010), *aff'd in part, rev'd in part*, 653 F.3d 1329 (Fed. Cir. 2011).

[13] *Id.* at 186.

[14] U.S. CONST. art. I, § 8, cl. 8.

[15] 702 F. Supp. 2d at 184.

[16] *Id.* at 232.

[17] *Id.* at 228.

[18] *Id.*

[19] *Id.* at 230.

state or thing."[20] The court dismissed Myriad's argument that the "analyzing" and "comparing" functions of the isolated DNA amounted to a transformation from its natural state, instead finding this process to be comparable to mere "data-gathering."[21] Additionally, the patent Myriad held on a process to compare the growth of cancer cells in the presence of different therapeutic substances was determined to merely involve the measuring of a basic scientific principle and was also deemed un-patentable. As such, both Myriad's DNA and method claims were held invalid.[22]

Upon review, the Federal Circuit reversed the district court's invalidation of the isolated DNA patents, affirmed the holding as to the method claim for comparing isolated gene sequences, and reversed on the process to compare growth of cancer cells claim.[23] Upon a grant of certiorari, the Supreme Court vacated the order and remanded to the Federal Circuit in light of its recent decision, *Mayo Collaborative Services v. Prometheus Laboratories Inc.*,[24] a case which, as discussed below, foreshadowed the final Supreme Court decision in *Myriad*.[25]

On its second hearing of the case, the Federal Circuit ultimately maintained its original position, holding the DNA claims and cancer-growth process patent-eligible but the methodology for observing the gene sequences patent-ineligible.[26] Finding both the isolated BRCA genes and the cDNA to have a different chemical structure from their original source DNA, the court determined these compositional claims fell within the scope of §101.[27] The court found that the products-of-nature exemption used by the lower court was too broad, as any product can be

---

[20] *Id.* at 233 (quoting *In re* Bilski, 545 F.3d 943, 954 (Fed. Cir. 2008)).

[21] *Id.* at 236.

[22] *Id.* at 238.

[23] Ass'n for Molecular Pathology v. U.S. Patent & Trademark Office, 653 F.3d 1329, 1357 (Fed. Cir. 2011).

[24] 132 S. Ct. 1289 (2012).

[25] Ass'n for Molecular Pathology v. Myriad Genetics, Inc., 132 S. Ct. 1794 (2012).

[26] Ass'n for Molecular Pathology v. U.S. Patent & Trademark Office, 689 F.3d 1303, 1336 (Fed. Cir. 2012).

[27] *Id.* at 1332–33.

traced back to a naturally occurring source.[28]

In regard to the cancer-growth process, the court noted that because the method included the "growing of host cells *transformed*" by an altered BRCA 1 gene or a cancer therapeutic, the claim on this process was patent-eligible under §101.[29] The transformative element distinguished this process from a mere comparison and analysis of cells.[30] Again, the court found no transformative process in the analysis of the BRCA sequences.[31] This claim, the court held, merely involved an abstract mental process, which could be accomplished by a simple inspection of the DNA.[32]

C. The Supreme Court's Decision

Following the Federal Circuit's opinion, the Supreme Court granted certiorari in November 2012 and prepared to hear the case on the merits. The Supreme Court issued its decision in June 2013. Justice Thomas, authoring the unanimous decision, did away with much of the complex scientific background and theories of §101, instead asking simply whether Myriad's patents assert a "new and useful . . . composition of matter" or merely a "naturally occurring phenomena."[33]

Rejecting the Federal Circuit's liberal application of transformation in the isolation of DNA, the Supreme Court found no significant change between the isolated BRCA genes and the genes in their original state.[34] The Court held that the discovery of an important and useful gene, no matter how groundbreaking or innovative, does not satisfy §101's new compositions requirement.[35]

In contrast, the Court held cDNA is not naturally occurring and

---

[28] *Id.* at 1331.
[29] *Id.* at 1335 (emphasis added).
[30] *Id.* at 1336.
[31] *Id.* at 1334.
[32] *Id.* at 1335.
[33] Ass'n for Molecular Pathology v. Myriad Genetics, Inc., 133 S. Ct. 2107, 2116 (June 13, 2013).
[34] *Id.* at 2117.
[35] *Id.*

is therefore patent-eligible.[36] Despite the cDNA strand containing the exons of its original source, the Court determined that this synthesized strand does not occur as a natural phenomenon. It is only producible in a lab setting.[37]

Finally, unlike in the previous decisions, the Court did not analyze the method claims. It did, however, suggest that had Myriad created an innovative way to manipulate an individual's genes in its search for the BRCA genes, a method patent could have been valid.[38] Here, since the processes for isolating the genes "were well understood, widely used, and fairly uniform insofar as any scientist engaged in the search for a gene would likely have utilized a similar approach," the Court found no such novel claim.[39]

Subsequent cases have generally followed the holding of *Myriad* closely, declining to explore the questions that remain.[40] This lack of exploration also means that the questions on the limits of naturally occurring product and method claims have not been completely answered. These unanswered questions provide a viable option for patent seekers: arguing that a once naturally occurring product exists only through man-made manipulation, even to the slightest extent, is enough to establish patentability.

II. AN EXAMINATION OF THE "NATURALLY OCCURRING PRODUCT" REQUIREMENT AS INTERPRETED BY THE SUPREME COURT

Though §101 appears on its face to be a straightforward rule, a deeper examination of its application reveals the statute's limitations that may still be exploited to a patent seeker's benefit. Justice Thomas relied heavily on the plain language of §101 in *Myriad*. However, as in *Mayo*, the Court again refused to define the contours of this section and when a product is no longer

---

[36] *Id.* at 2119.
[37] *Id.*
[38] *Id.* at 2119–20.
[39] *Id.*
[40] *See* Ariosa Diagnostics, Inc. v. Sequenom, Inc., No. C11-06391 SI, 2013 WL 5863022 (N.D. Cal. Oct. 30, 2013); Oleksy v. General Elec. Co., No. 06 C 01245, 2013 WL 3233259 (N.D. Ill. June 26, 2013).

considered "naturally occurring." This section will introduce the challenges and shortcomings within the statute itself and the court-created limitations.

A. Statutory Shortcomings

The statute in question, 35 U.S.C. §101, does not provide specific guidance on the limits of patent-eligibility. Rather, the statute reads, "Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title."[41] Based on only the statute's plain language, the *Myriad* opinion is troubling since Myriad did *discover* a new and useful process. Yet the discovery did not satisfy the statutory standard. Additionally, Myriad isolated the BRCA genes for testing, but again this was not a valid "new or useful improvement." Thus, on the face of the case, Myriad appeared to have satisfied the discovery requirement. The Supreme Court's decision reveals, however, that a patent seeker cannot rely on the plain language of §101 alone. As guidance through the Court's interpretation, the patent seeker must also consider the common law exceptions to the statute.

B. Interpreting the Statute's Court-Created Limits

Recognizing that certain items and phenomena cannot truly be "created" for the purposes of patents, the Supreme Court gradually identified three subjects over time that are not patentable under §101: (1) laws of nature; (2) natural phenomena; and (3) abstract ideas.[42] However, the Court has also realized that these exceptions cannot be overly broad. Since nearly every invention or theory will rely on either a law of nature, natural phenomenon, or abstract idea, the possibility of "eviscerating" patent law must constantly be kept in mind.[43] At some point the creative manipulation of a law of

---

[41] 35 U.S.C. § 101 (1952).

[42] Diamond v. Diehr, 450 U.S. 175, 185 (1981).

[43] Mayo Collaborative Servs. v. Prometheus Labs, Inc., 132 S. Ct. 1289, 1293 (2012).

nature, natural phenomena, or abstract idea will need to be protected under patent law. The Court declined to specify where the line is drawn between the exceptions to §101 and the eviscerating, overly-broad interpretations. The *Myriad* opinion, however, hints at when a patented natural product falls within the realm of patentability.

III. CREATING VIABLE PATENT CLAIMS POST-*MYRIAD*

Despite the Supreme Court issuing a very blunt and fairly straightforward decision in *Myriad*, the Court alluded to the contours of the Court-created limits of §101 as well as unaffected arguments. In the case, Myriad's arguments about the usefulness of its discovery and difficulty in isolating the BRCA genes were not enough to satisfy §101. The opinion appears on its face to be so broad and insensitive to the nuances of Myriad's claims that it created a sweeping bar against patenting any natural materials. However, an analysis of the cDNA claims, application rules, and policy concerns reveals that the Court left room for arguments to circumvent the basic natural products rule, which the careful attorney can utilize in drafting, defending, or challenging patent claims.

A. Deciphering the Limits of New and Useful Improvements through cDNA

As noted above, §101 poses a difficult dilemma for patent seekers. Natural products cannot be patented, but since everything comes from a natural product, what constitutes enough manipulation of the natural state to qualify as a patentable product under §101? The Court's short analysis of cDNA suggests that the required transformation from natural to unnatural may in fact be minimal.

Immediately following *Myriad*, the United States Patent and Trademark Office issued a memorandum to its staff directing examiners to reject product claims "drawn solely to naturally occurring nucleic acids or fragments thereof, whether isolated or

not . . . ."[44] However, the Office recognized that claims demonstrating that the naturally occurring matter has been altered ("e.g., a man-made variant sequence") are eligible.[45] The Office later issued additional guidance to the Patent Examining Corps, directing that all claims that recite or involve a law of nature, natural phenomenon, or natural product be rejected unless the claims also recite something "significantly different" than the judicial exception.[46] The Office suggested two general ways in which a significant difference can manifest: (1) the claim adds elements or steps to the judicial exception that "practically apply the judicial exception in a significant way" or (2) the claim states some features or steps demonstrating the claimed subject matter is "markedly different" from the natural product or phenomena.[47] Additionally, the Office listed six factors that suggest a claim is eligible and six that suggest it is ineligible. Two of these factors are of particular relevance to patent claims involving genetic material: "factor (a)," where the claim is a product that appears to be merely a natural product but demonstrates that it is non-naturally occurring and markedly different from the natural product (weighing in favor of eligibility), or "factor (g)," where the claim recites a natural product or something that resembles a natural product but is not markedly different.[48] Thus, in applying for a patent, the most significant step an applicant can take is stressing the variation that has occurred to the natural product. However, these guidance memos do little to clarify what constitutes a marked or significant difference in the claimed product.

Rather, a determination of the degree necessary to satisfy this

---

[44] Memorandum from Andrew H. Hirshfeld, Deputy Comm'r for Patent Examination Policy, U.S. Patent and Trademark Office, to the Patent Examining Corps (June 13, 2013), *available at* http://www.uspto.gov/patents/law/exam/myriad_20130613.pdf.

[45] *Id.*

[46] Memorandum from Andrew H. Hirshfeld, Deputy Comm'r for Patent Examination Policy, U.S. Patent and Trademark Office, to the Patent Examining Corps (Mar. 14, 2014), *available at* http://www.uspto.gov/patents/law/exam/myriad-mayo_guidance.pdf.

[47] *Id.* at 3–4.

[48] *Id.* at 4.

"significantly different" standard is best clarified by the *Myriad* decision and previous natural product cases. Central to the Court's rejection of Myriad's BRCA patents was the idea that the company had not made any new or useful improvements to the original gene sequence.[49] The BRCA genes isolated from the individual's DNA were structurally the same product as the genes in their natural state. Conversely, the Court in *Diamond v. Chakrabarty* found that when scientists added plasmids to a bacterium, which broke down various components of a bacterium, the resulting bacterium was patentable.[50] The process of breaking down the bacterium was not the claim in dispute, but the resulting product was.[51] The Court found that the final bacterium was the result of "human ingenuity," having "a distinctive name, character [and] use."[52] Thus, *Chakrabarty* indicates that the final product resulting from the natural reaction between two other natural products meets the patentability standard.

While the extent of the change has not been defined, the *Myriad* Court's examination of the cDNA claims provides insight on how little the change really needs to be. The Court found that cDNA easily meets the threshold for §101, despite the petitioner's arguments that the basic structure of cDNA is "dictated by nature, not by the lab technician."[53] Since the exon-only sequence does not occur in nature, the Court found the cDNA patents to be valid.[54] The holdings of *Myriad* and *Chakrabaty* suggest that all that is required to meet the new and useful improvement standard for natural products is a change that could not occur but for the patent seeker's intervention or process.

Without any firm measurement by the Court, even the slightest variation could meet the standard under §101 as long as the change does not occur as a natural process. Litigators defending or challenging future patent claims on similar grounds should seize

---

[49] Ass'n for Molecular Pathology v. Myriad Genetics, Inc., 133 S. Ct. 2107, 2117 (June 13, 2013).

[50] 447 U.S. 303, 309–10 (1980).

[51] *Id.*

[52] *Id.*

[53] 133 S. Ct. at 2119.

[54] *Id.*

upon this ambiguity, stressing the uniqueness of the holder's claims, or lack thereof. In particular, focus should be drawn to the differences between the naturally occurring state and the processed result.

While Myriad relied heavily on its discovery of the BRCA genes, the Court's decision and the Patent Office's subsequent guidance documents may result in a shift away from the discovery arguments. Discovery, no matter how groundbreaking, is merely a noteworthy accomplishment that affords little legal protection post-*Myriad*. Instead of attempting to protect their discovery, patent seekers will likely find more success arguing the validity of the resulting product. Patent seekers might even forgo method claims, especially those involving well-known scientific processes, and stress the new and useful improvements on a naturally occurring product in their patent requests.

B. "Application of New Processes" Patents Remain Valid

Patent seekers should also not ignore the importance of making application claims, an opportunity the Supreme Court and Federal Circuit each believed Myriad had squandered.[55] The Supreme Court suggested that Myriad was in an advantageous position to claim new applications of its knowledge about BRCA 1 and 2.[56] The Federal Circuit noted that Myriad could claim application of the BRCA discoveries especially in its fight against breast cancer.[57] However, to a future patent seeker, an application claim will be easier said than done. The claim will have to state a specific application of the discovery, but such a statement does not guarantee that the discovery, process, or modified product will be protected by patent law.[58] Practitioners should keep in mind that

---

[55] *Id.* at 2120; Ass'n for Molecular Pathology v. U.S. Patent & Trademark Office, 689 F.3d 1303, 1349 (Fed. Cir. 2012).

[56] 133 S. Ct. at 2120 (quoting 689 F.3d at 1349).

[57] 689 F.3d at 1349.

[58] *See* Memorandum from Andrew H. Hirshfeld, Deputy Comm'r for Patent Examination Policy, U.S. Patent and Trademark Office, to the Patent Examining Corps (Mar. 14, 2014), *available at* http://www.uspto.gov/patents/law/exam/myriad-mayo_guidance.pdf (stating that a natural product claim can be analyzed with only factors (a) and (g) while other claims, including

the Court separated the application claims from the product claim.[59]

For example, in *Myriad*, while the BRCA genes could never have been patentable, the patent claim would be acceptable had it made a new or useful application claim. Conversely, one could make a valid patentable product claim, but the claim for the application of the product, if relying upon well-known processes, would not be eligible. Thus the patent seekers should recognize that product and application claims are not necessarily bound together and that a claim for application may still protect discovery even if the product claim is deemed ineligible.

C. Limits of the Exceptions: How Far Is Too Far?

If significant changes to a product of nature are impractical or impossible and an application claim is futile, a policy argument still remains a powerful tool in defending a patent. Though the Supreme Court raised the issue of whether an overly broad reading of §101 will detrimentally impact future patent claims, the line is yet to be definitively drawn. Though such arguments have no place in applications for patents, this issue will continue to be an important argument for the courtroom.

One important aspect of the policy argument is the difficulty of discovery. Even the Supreme Court missed the opportunity to distinguish between easily made discoveries of natural products, phenomenon, or abstract ideas and discoveries that involve a far more nuanced approach. The strict adherence to the plain language of §101 does not allow for such distinctions. In *Mayo*, decided shortly before the final *Myriad* decision, the Court equated (at least in terms of patent eligibility) medical discoveries to discoveries based on basic observations, noting that "a new plant found in the wild is not patentable subject matter."[60] Unlike a person who stumbles upon a plant and discovers it has medicinal purposes through mere chance, genetics is a very deliberate and expensive

---

application claims, should be analyzed with the remaining factors).

[59] 133 S. Ct. at 2119.

[60] Mayo Collaborative Servs. v. Prometheus Labs, Inc., 132 S. Ct. 1289, 1293 (2012).

science. Individuals do not merely come across genes in the course of their day. Trained scientists with advanced equipment and funding make concentrated efforts to seek out such phenomena. Yet the Court refused to make such a distinction and essentially held the geneticist's discovery to the same standard as the lucky individual who discovers the plant.

Another issue is the potential chilling effect on the biotech industry. The basic principles of patent law are that patent law needs first to seek to "foster and reward" inventor and second to promote disclosure of inventors' ideas to stimulate further innovations.[61] As the field of genetics continues to grow, the courts will have to continue to keep these principles in mind. While patient rights will always remain a valid concern, the fostering of scientific discovery should not be ignored. In light of the broad holding of *Myriad*, this public policy argument against stifling discovery may carry increasing weight and, as such, courts may be reticent to remove protections for innovative discoveries.

CONCLUSION

Given the relatively recent publication of *Myriad*, application of the case has been slow in lower courts. Nonetheless, the importance and profitability of scientific, and specifically genetic, research requires that the courts draw a line so as to not completely stifle the field. However, this need must be balanced with patient rights. The *Myriad* decision offers insights into both these arguments. As long as a claim attempts to patent genetic material in its natural state, the courts will invalidate the patent for the foreseeable future. However, the validation of the cDNA patents suggests that even the slightest changes to the natural state can suffice for patentability under §101. Additionally, *Myriad* does not appear to have had an effect on method or application claims. Thus, practitioners are still left with the ability to patent genetic materials as long as the claim places emphasis on variations on the product, method, or unique application of a process. Finally, the

[61] Robert A. Matthews Jr., 1 Annotated Patent Digest §1:2: Purposes of the patent system (updated July 2014).

public policy argument against overly broad interpretations of §101 can continue to be argued with attention to the necessity for protection and promotion of discovery.

PRACTICE POINTERS

- Keep in mind policy arguments about the overreach of the law and argue the necessity of protecting and promoting innovation.
- When drafting a patent application, stress that the new product cannot occur in nature and only exists through the process rendered by the patent seeker.
- Put additional emphasis on the description of utility and the transformative elements of the inventive method or composition as an application of a natural law.
- Avoid claims that only have "comparing" or "determining" elements associated with a natural correlation.

WASHINGTON JOURNAL OF LAW, TECHNOLOGY & ARTS
VOLUME 10, ISSUE 1 SUMMER 2014

SPYING ON AMERICANS: AT WHAT POINT DOES THE NSA'S COLLECTION AND SEARCHING OF METADATA VIOLATE THE FOURTH AMENDMENT?

Elizabeth Atkins[*]

Cite as: 10 Wash. J.L. Tech. & Arts 51 (2014)
http://digital.lib.washington.edu/dspace-law/handle/1773.1/1390

ABSTRACT

Edward Snowden became a household name on June 5, 2013, when he leaked highly classified documents revealing that the American Government was spying on its citizens. The information exposed that the National Security Agency (NSA) collected millions of American's metadata through forced cooperation with telephone-service providers. Metadata contains sensitive and private information about a person's life. When collected and searched, metadata can reveal a portrait of a person's intimate activities amounting to a violation of one's reasonable expectation of privacy.

This Article suggests changing the current standard allowing the NSA to collect and search metadata under Section 215 of the USA PATRIOT Act. The threshold needed to obtain and search a person's metadata should be raised from the current standard of reasonable and articulable suspicion to a higher burden of probable cause. Since Mr. Snowden's unauthorized disclosure, there has been public outcry regarding metadata collection. In response, President Obama issued a Public Policy Directive limiting the scope of metadata that the NSA can collect. Additionally, Congress has proposed legislation changing how the NSA collects, stores, and searches

---

[*] Elizabeth Atkins, Thomas Jefferson School of Law, Class of 2015. Thank you to Professor Cohn for her valuable insight and expertise, and to Randy Abreu for his patience and infinite support.

metadata. The bills, however, keep intact the minimum reasonable and articulable standard necessary to search metadata.

The breadth of information that can be gleaned from metadata makes it intrusive and subjects it to the Fourth Amendment. Yet gathering and searching metadata can be a valuable tool in the fight against terrorism and protecting American citizens from future attacks. Requiring the threshold to be raised to a probable cause determination adequately balances privacy interests against national security interests.

TABLE OF CONTENTS

INTRODUCTION

> "Metadata is what allows an actual enumerated understanding, a precise record of all the private activities in all of our lives. It shows our associations, our political affiliations and our actual activities."[1]

---

[1] Edward Snowden, Remarks at the Amnesty International USA Annual General Meeting (Apr. 5, 2014); *see* Karl Plume, *Snowden, Greenwald urge caution of wider government monitoring at Amnesty event*, REUTERS (Apr. 5, 2014, 8:29 PM), http://www.reuters.com/article/2014/04/06/us-usa-security-

On June 5, 2013, Edward Snowden shocked the world when he revealed highly classified National Security Agency (NSA) documents to *The Guardian*, a British daily newspaper.[2] These documents exposed the Foreign Intelligence Surveillance Court's (FISC) secret order instructing Verizon to collect metadata from all telephone calls within the United States and abroad.[3] Snowden disclosed that the NSA was spying on American citizens through the mass collection of "telephony metadata," with Congressional and Presidential authorization.[4] Immediately thereafter, President Obama and Senator Diane Feinstein began downplaying the Orwellian nature of the program, notably justifying it by stating: "*it's just metadata*."[5]

However, the mass collection of metadata was troubling to many Americans because the NSA was not only spying on those believed to be associated with Al-Qaida but also on messages between Americans without ties to suspected terrorism.[6] Even

---

snowden-idUSBREA3500320140406.

[2] Glenn Greenwald, *NSA collecting phone records of millions of Verizon customers daily*, THE GUARDIAN (June 5, 2013), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

[3] Marjorie Cohn, *NSA Metadata Collection: Fourth Amendment Violation*, JURIST (Jan. 15, 2014), http://jurist.org/forum/2014/01/marjorie-cohn-nsa-metadata.php; Administration White Paper, *Bulk Collection of Telephony Metadata Under Section 215 of the USA PATRIOT Act* 1–2 (Aug. 9, 2013), *available at* http://op.bna.com/der.nsf/id/sbay-9aeu73/.

[4] In re Application of the FBI for an Order Requiring the Prod. of Tangible Things From [REDACTED], No. BR 13–80, 2013 U.S. Dist. LEXIS 147002 (FISA Ct. Apr. 25, 2013) [hereinafter Primary Order]; Greenwald, *supra* note 2.

[5] President Obama, Remarks by the President on Review of Signals Intelligence (Jan. 17, 2014), available at http://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence [hereinafter President Obama's Remarks]; *Transcript: Diane Feinstein, Saxby Chambliss, Explain, Defend NSA Phone Records Program*, WASH. POST (June 6, 2013), http://www.washingtonpost.com/blogs/post-politics/wp/2013/06/06/transcript-dianne-feinstein-saxby-chambliss-explain-defend-nsa-phone-records-program [hereinafter *Senator Feinstein's Remarks*]; *see, e.g.*, ALDOUS HUXLEY, BRAVE NEW WORLD (1932); GEORGE ORWELL, ANIMAL FARM (1945); GEORGE ORWELL, NINETEEN EIGHTY-FOUR (1949). These books popularized the concept that would come to be known as "Orwellian", which describes manipulation of citizens by a totalitarian government by use of secret surveillance.

[6] *Id.*; James Ball, *NSA Monitored calls of 35 world leaders after US official*

more disturbing was the massive amount of sensitive and personal information that could be gathered from metadata in and of itself.[7] As metadata became defined in the public sphere, it became clear to Americans and human rights organizations alike that it's not *just* metadata.

The NSA's sweeping surveillance was legalized when Congress passed the USA PATRIOT Act, arguably the most expansive piece of legislation in America's history.[8] Post-9/11, the USA PATRIOT Act allowed the government to use surveillance and technology more aggressively than ever before in an attempt to prevent future attacks.[9]

Congress originally authorized metadata collection under Section 215 of the Act.[10] Section 215 was amended in the USA PATRIOT Improvement and Reauthorization Act of 2005, which required the government to provide "a statement of facts showing that there are reasonable grounds to believe that the tangible objects sought are relevant . . . against international terrorism . . . ."[11] Section 215 expanded the government's ability to compel the

---

handed over contacts, THE GUARDIAN (Oct. 24, 2013), http://www.theguardian.com/world/2013/oct/24/nsa-surveillance-world-leaders-calls; *see* Josh Levs & Catherine E. Shoichet, *Europe furious, 'shocked' by report of U.S. spying*, CNN.COM, (July 1, 2013), http://www.cnn.com/2013/06/30/world/europe/eu-nsa (explaining that European officials are shocked and outraged by the reports Snowden leaked that the NSA is spying on European Union leaders).

[7] *See infra* Part IV.

[8] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), 107 Pub. L. No. 56, § 215, 115 Stat. 272, 287–88 (2001) (codified in scattered titles of U.S.C.); Drew Fennell, *The USA PATRIOT Act*: *Can we be Both Safe and Free?*, 21 DEL. LAW. 10, 10 (2003) ("On October 25, 2001, a matter of weeks after September 11, the U.S. Congress passed the USA PATRIOT Act, a bill that contains the most sweeping and comprehensive changes in domestic law enforcement in history . . . .").

[9] Richard A. Clarke et al., THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES, LIBERTY AND SECURITY IN A CHANGING WORLD 73 (Dec. 12, 2013) [hereinafter PRESIDENT'S REVIEW GROUP REPORT].

[10] USA PATRIOT Act § 215.

[11] USA PATRIOT Improvement and Reauthorization Act of 2005, 120 Stat. 196 § 106 (codified as amended at 50 U.S.C. § 1861(b)(2)(A)).

production of "any tangible things including books, records, papers, documents, and other items."[12]

Under this expanded program, the government began collecting United States citizens' call records without warrants. This program is unprecedented because it targeted not only phone calls made to suspects living outside of the country but call records *between American citizens* themselves. The government systematically collected and searched sensitive information on its own citizens without meeting the constitutional constraints of the Fourth Amendment. In most cases, the Fourth Amendment imposes a warrant requirement to perform a search.[13] Prior to performing a search on a constitutionally protected area, a person must first have probable cause and then obtain a warrant from a judge.[14] The government's failure to obtain a warrant before searching a person's metadata records violates that person's reasonable expectation of privacy.[15] Even though government officials, including President Obama, have reassured American citizens that they are not listening to the content of their calls, the metadata of these calls can still reveal an illuminating look at the callers' private lives.

For example, consider Person X, an American citizen born in the United States. Person X is a college-educated, 26-year-old program developer who just began law school. He has no association to terrorist activity. Yet every day the NSA collects his phone records and stores all of his metadata in a database waiting to be queried.

Imagine one day the NSA suspects that Person X is associated with a terrorist organization. Every phone number he has contacted within the past five years is collected. The information the government could collect about Person X based solely on his metadata displays detailed information about his life: the abortion clinic he called in college after an accident with his girlfriend, his pastor and religious affiliation, his therapist, his association with the National Rifle Association, the presence of bill collectors, a

---

[12] PRESIDENT'S REVIEW GROUP REPORT, *supra* note 9, at 81.
[13] Katz v. United States, 389 U.S. 347 (1967).
[14] *Id.*
[15] *Id.*

clinic that treats sexually transmitted diseases, or the pizza restaurant down the street from his house from which he orders. Suddenly, what seems like an innocent and harmless amount of "metadata," coupled with simple investigation, becomes an intimate look into the personal life of Person X. The government has no right to this level of private information about a person, absent a warrant as required by the Fourth Amendment. Yet the government collects this data on U.S. citizens on a daily basis.

Part I of this Article provides an in-depth background of the development of the right to privacy with respect to modern technology and surveillance. Part II discusses the history that led to the passage of the USA PATRIOT Act, particularly Section 215, which authorizes metadata collection. Part III discusses current challenges to the metadata collection program. Part IV argues that the threshold to search metadata under Section 215 should be raised from a reasonable articulable suspicion of terrorist activity to the higher standard of probable cause.

I. THE HISTORY OF MODERN SURVEILLANCE DEVELOPED UNDER THE FOURTH AMENDMENT

Modern surveillance can be traced to the Cold War era; specifically, to the Vietnam War.[16] Former Presidents Lyndon Johnson and Richard Nixon encouraged expansive surveillance of individuals and organizations opposed to the war.[17] As a result, the CIA began monitoring antiwar activists.[18] In the 1950s, FBI Director J. Edgar Hoover conducted a massive counter-intelligence program, known as COINTELPRO.[19] Under the guise of fighting communism, the government engaged in surveillance, infiltration, dissemination of false information, and abuse of the criminal justice system.[20] In the 1970s, a series of congressional committees

---

[16] PRESIDENT'S REVIEW GROUP REPORT, *supra* note 9, at 54.

[17] *Id.* at 54–55.

[18] *Id.*

[19] Natsu Taylor Saito, *Whose Liberty? Whose Security? The USA PATRIOT Act in the Context of COINTELPRO and the Unlawful Repression of Political Dissent*, 81 OR. L. REV. 1051, 1080–88 (2002).

[20] *Id.*

convened to discuss what led to the abuses that had taken place under COINTELPRO during the previous decades.[21]

The final report, containing 96 policy recommendations, was prepared by the Church Committee, named after Chairman Senator Frank Church.[22] The Church Committee Report concluded that spying endangers both the security of the nation and the rights of Americans.[23] In 1976, President Gerald Ford formally prohibited the CIA from using surveillance measures on American citizens unless explicitly approved by the Attorney General.[24] The use of electronic surveillance for national security purposes became a growing concern, culminating in a series of privacy cases.[25] These cases governed the way courts have viewed electronic data for more than 40 years.[26]

A. The Court's Development of a Right to Privacy in Emerging Technology

Three Supreme Court cases have helped shape the right to privacy in light of emerging technological advancements.[27] The invention of electronic devices led to the discovery of how to eavesdrop on communications that use these devices. The police turned to wiretapping to monitor otherwise private conversations in

---

[21] *Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities of the United States Senate*, 94th Cong. (1976) [hereinafter *Church Committee Report*].

[22] Nicholas C. Dranias, *The Patriot Act of 2001 versus the 1976 Church Committee Report: An Unavoidable Clash of Fundamental Policy Judgments*, 17 C.B.A. REC. 28, 29 (2003).

[23] *Id.* at 30.

[24] Exec. Order No. 11905, United States Foreign Intelligence Activities, 41 Fed. Reg. 7703 (Feb. 18, 1976).

[25] *See, e.g.*, Olmstead v. United States, 277 U.S. 438, 478 (1928), *overruled by* Katz v. United States, 389 U.S. 347 (1967), *and* Berger v. New York, 388 U.S. 41 (1967); Katz v. United States, 389 U.S. 347 (1967); Miller v. United States, 425 U.S. 435 (1976); Smith v. Maryland, 442 U.S. 735 (1979); United States v. Jones, 132 S. Ct. 945 (2012).

[26] *See, e.g.*, *Olmstead*, 227 U.S. at 478; *Katz*, 389 U.S. 347; *Miller*, 425 U.S. 435; *Smith*, 442 U.S. 735; *Jones*, 132 S. Ct. 945 (cases cited range from 1928 to 2012).

[27] *See Olmstead*, 277 U.S. 438; *Katz*, 389 U.S. 347; *Jones*, 132 S. Ct. 945.

order to collect evidence against suspected criminals. Those people whose conversations were overheard challenged the collection of such data, and the debate over privacy rights through electronic communications began. *Olmstead v. United States*, *Katz v. United States*, and *United States v. Jones* all involve electronic surveillance and the right to privacy under the Fourth Amendment.[28]

1. *Olmstead v. United States*: Establishing Privacy as a Trespassory Doctrine

In *Olmstead*, federal agents installed wiretaps on phone lines to investigate a conspiracy to distribute alcohol during the Prohibition.[29] The agents tapped phone lines leading into the suspects' houses and offices without actually entering the premises.[30] They gathered evidence for five months and recorded multiple conversations.[31] The Supreme Court held that a wiretap was not a "search" within the meaning of the Fourth Amendment because there was not a physical trespass onto real property.[32] This holding paved the way for the trespassory/non-trespassory distinction regarding invasions into constitutionally protected areas.[33] However, as people increasingly relied on the telephone for conducting their private affairs, *Olmstead's* reasoning became more difficult to maintain.[34]

Indeed, Justice Louis Brandeis' dissent in *Olmstead* has become the flagship of privacy rights arguments in post-*Olmstead* cases.[35] Justice Brandeis disagreed with the majority's distinction

---

[28] *Olmstead*, 277 U.S. 438; *Katz*, 389 U.S. 347; *Jones*, 132 S. Ct. 945.

[29] *Olmstead*, 277 U.S. at 455–58 (describing the factual background of the case).

[30] *Id.*

[31] *Id.* at 471 (Brandeis, J., dissenting).

[32] *Id.* at 466.

[33] Lon A. Berk, *After Jones, The Deluge: The Fourth Amendment's Treatment of Information, Big Data and the Cloud*, 14 J. HIGH TECH. L. 1, 12 (2014).

[34] *Id.* at 13.

[35] Neil M. Richards, *The Puzzle of Brandeis, Privacy, and Speech*, 63 VAND. L. REV. 1295, 1296 (2010).

between trespassory and non-trespassory invasions.[36] He stated that unjustified searches and seizures violate the Fourth Amendment no matter how the information was gathered.[37] The principles set forth in the majority, Brandeis reasoned, go to the very nature of "constitutional liberty and security" and apply to all invasions by the government.[38] What violates a person's personal liberty is not the actual rummaging of drawers, but the "invasion of his indefeasible right of personal security," Brandeis wrote.[39] In comparing wiretapping to mail tampering, Brandeis thought that the invasion of the telephone was far worse.[40] When a telephone line is tapped, confidential conversations are heard and privacy is violated at both ends of the line.[41]

2. *Katz v. United States*: Overruling *Olmstead* and Paving the Way toward Non-Trespassory Privacy Rights

In 1967 the Supreme Court finally adopted a different test for determining whether a search was reasonable, relying principally on the Brandeis dissent in *Olmstead*.[42] In *Katz v. United States*, Katz was a bookmaker who used a telephone booth to transmit wagering information across state lines.[43] Federal agents used an electronic listening device outside of the telephone booth and obtained recordings of the calls.[44] The recordings were used at trial to convict Katz.[45] On appeal, the government based its argument on the trespassory view of the Fourth Amendment, noting that the agents were outside of the phone booth and not within a

---

[36] *Olmstead*, 277 U.S. at 477–78 (Brandeis, J., dissenting).

[37] *Id.* ("Unjustified search and seizure violates the Fourth Amendment, whatever the character of the paper; whether the paper when taken by the federal officers was in the home, in an office, or elsewhere; whether the taking was effected by force, by fraud, or in the orderly process of a court's procedure.").

[38] *Id.* at 474 (quoting Boyd v. United States, 116 U. S. 616).

[39] *Id.* at 475 (quoting Boyd v. United States, 116 U. S. 616).

[40] *Id.* at 475.

[41] *Id.*

[42] *See* Katz v. United States, 389 U.S. 347, 353 (1967).

[43] *Id.* at 348.

[44] *Id.* at 348–54.

[45] *Id.* at 348.

constitutionally protected area.[46]

The Supreme Court rejected this argument and overruled the literal interpretation of *Olmstead*, recognizing that the Fourth Amendment "protects people not places."[47] Specifically, the Court stated that telephone technology had become "vital" to private communications and rejected the argument that the use of a telephone was analogous to a broadcast of one's voice into public areas.[48] The Justices reasoned that the Fourth Amendment protects people, not simply areas, and a violation of the Fourth Amendment cannot turn on the presence or absence of a physical intrusion.[49]

Justice John Harlan's concurrence built upon the framework set forth in the majority opinion.[50] He formulated the "reasonable expectation" test for determining whether government activity constitutes a violation of the Fourth Amendment.[51] The two-prong test requires that (1) the individual has an actual (subjective) expectation to privacy, and (2) the expectation is one society is prepared to recognize as "reasonable."[52] If both prongs are satisfied, there is a reasonable expectation of privacy.[53] Harlan's test, and not the majority opinion, was adopted in *Smith v. Maryland* and is the test now used to determine whether a search has taken place.[54]

3. *United States v. Jones*: Foreshadowing Modern Non-Trespassory Privacy Concerns

In 2010 the Supreme Court unanimously held that tracking a person's movements for a month via a GPS monitoring device that police had attached to the driver's vehicle without a warrant

---

[46] *Id.* at 352.
[47] *Id.* at 351.
[48] *Id.* at 352.
[49] *Id.* at 353.
[50] *Id.* at 361 (Harlan, J., concurring).
[51] *Id.* at 360–61.
[52] *Id.* at 361.
[53] *Id.*
[54] Peter Winn, *Katz and the Origins of the "Reasonable Expectation of Privacy" Test*, 40 MCGEORGE L. REV. 1, 7 (2009).

violates the Fourth Amendment.[55] In *United States v. Jones*, federal agents were investigating Mr. Jones for narcotics distribution and placed a GPS device under his Jeep without a warrant.[56] For the next 28 days, agents used the device to track the Jeep and collected more than 2,000 pages of data.[57]

Jones was convicted after the trial court found that his Fourth Amendment rights were not violated since there was no reasonable expectation of privacy in movements from one place to another.[58] On appeal, the Supreme Court found that a "reasonable person does not expect anyone to monitor and retain a record of every time he drives his car . . . rather, he expects his movements to remain 'disconnected and anonymous.'"[59] The Supreme Court's opinion was not based on the *Katz* reasonable expectation of privacy test, but instead relied on the *Olmstead* analysis regarding common law trespass.[60]

B. Smith v. Maryland*: Developing the Third-Party Doctrine*

The third-party doctrine further confuses a person's privacy rights when electronic devices are involved. In *Smith v. Maryland*, the Supreme Court held that one who gives information to a third-party does not have a reasonable expectation of privacy, and thus falls outside the purview of the Fourth Amendment.[61]

In *Smith*, the defendant Smith was convicted of robbery after the police instructed the telephone company to monitor the phone numbers Smith dialed. [62] After the victim was robbed, she gave

---

[55] United States v. Jones, 132 S. Ct. 945, 949 (2012).
[56] *Id.* at 948.
[57] *Id.*
[58] *Id.*
[59] United States v. Maynard, 615 F.3d 544, 561 (D.C. Cir. 2010) (quoting United States v. Wylie, 569 F.2d 62, 6 (D.C. Cir. 1977)) ("[P]olice-citizen communications which take place under circumstances in which the citizen's 'freedom to walk away' is not limited by anything other than his desire to cooperate do not amount to 'seizures' of the person."), *cert. denied* 131 S. Ct. 671 (2010), *aff'd*, *Jones*, 132 S. Ct. 945.
[60] *Jones*, 132 S. Ct. at 953.
[61] Smith v. Maryland, 442 U.S. 735, 742 (1979).
[62] *Id.* at 737.

police a description of the attacker and of an automobile parked near the scene.[63] She also began receiving threatening phone calls from the same attacker.[64] Eleven days later, a police officer spotted a man matching the description provided by the victim driving the same automobile.[65] The police officer traced the license plate to Michael Smith.[66] The next day the telephone company, at the request of the police department, installed a pen register at its main office to record the numbers dialed from Smith's telephone.[67] The police did not have a warrant before the company installed the pen register.[68] The register revealed Smith had called the victim after the robbery, permitting police to obtain a warrant to search his home.[69] Smith was arrested based on evidence gathered in his home and afterwards he was positively identified by the victim as her attacker.[70]

During pre-trial motions, Smith sought to suppress all evidence derived from the pen register, claiming the pen register violated his Fourth Amendment right to privacy because the police failed to obtain a warrant.[71] The trial court denied the motion and after Smith was convicted, he appealed.[72] The court of appeals affirmed the conviction, holding that "there is no constitutionally protected reasonable expectation of privacy in the numbers dialed into a telephone system and hence no search within the fourth amendment [sic] is implicated by the use of a pen register installed at the central offices of the telephone company."[73] Three judges dissented, one stating that individuals do have a legitimate expectation of privacy in the phone numbers they dial and concluding that the pen register was a search.[74]

---

[63] *Id.*
[64] *Id.*
[65] *Id.*
[66] *Id.*
[67] *Id.*
[68] *Id.*
[69] *Id.*
[70] *Id.*
[71] *Id.*
[72] *Id.* at 737–38.
[73] *Id.* at 738 (quoting Smith v. State of Maryland, 283 Md. 156, 173 (1978)).
[74] *Id.* at 738.

The Supreme Court first quoted *Katz v. United States* in defining what constitutes a "search" under the Fourth Amendment.[75] The Court noted the difference between *Katz* and the pen register used against Smith.[76] In *Katz* the police used a device to listen to the content of the defendant's conversation. [77] In *Smith*, the police only obtained a telephone number.[78] The Supreme Court held that there is no reasonable expectation of privacy in the numbers dialed from a phone because the user voluntarily dials the numbers and conveys the information to the telephone company.[79] The justification for this holding was twofold. First, the Court doubted that "people in general entertain any actual expectation of privacy in the numbers they dial."[80] Second, the Court wrote that even if Smith did have an expectation of privacy in the numbers he dialed, it was not one that society was willing to recognize as reasonable.[81] This was based on the Court's previous holdings that there is no legitimate expectation of privacy in information disclosed to a third party.[82]

Three of the Justices dissented, believing that Smith had a right to privacy in the phone numbers he dialed, and that the pen register did constitute a search under the Fourth Amendment.[83] Justice Thurgood Marshall wrote, "Privacy is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes."[84] There was no way for the Supreme Court to know its ruling would become the justification for the metadata

---

[75] *Id.* at 739–40.
[76] *Id.* at 740.
[77] *Id.*
[78] *Id.*
[79] *Id.* at 745.
[80] *Id.* at 742.
[81] *Id.* at 743–44.
[82] *Id.* at 744 (citing United States v. Miller, 425 U.S. 435, 442–444; Couch v. United States, 409 U.S. 322, 335–36; United States v. White, 401 U.S. 745, 752 (plurality opinion); Hoffa v. United States, 385 U.S. 293, 302 (1966); Lopez v. United States, 373 U.S. 427 (1963)).
[83] *Smith*, 442 U.S. at 746–52 (Stewart, Brennan, Marshall, JJ., dissenting).
[84] *Id.* at 740.

collection program. Yet the three dissenting Justices foreshadowed the exact issue that is currently the subject of public debate: whether society is ready to recognize a right to privacy in metadata collected under Section 215 of the USA PATRIOT Act.

II. ENACTMENT OF THE USA PATRIOT ACT

Two pieces of legislation led to the metadata program under Section 215. The first is the Foreign Intelligence Surveillance Act of 1979, and the second is the USA PATRIOT Act, which has been amended several times since its inception in 2001.[85] The last amendment expanded Section 215, which allowed the collection of metadata as revealed by the Snowden disclosures in 2013.[86]

A. The Foreign Intelligence Surveillance Act of 1978: Wiretapping and Foreign Intelligence Surveillance

In order to implement the recommendations of the Church Committee Report, Congress enacted the Foreign Intelligence Surveillance Act ("FISA") of 1978.[87] One of FISA's goals was to reconcile the Church Committee's concerns for protecting people against the abuse of power documented in the 1970's with the preservation of the government's ability to protect itself from foreign threat.[88] Although *Katz* held that the Fourth Amendment prohibited the government from wiretapping without a warrant if the interception would produce *evidence of criminal conduct*, it remained unclear whether the same was true when the government investigated "activities of foreign power."[89]

FISA was designed to address these questions, and its creation involved strict rules and structured oversight by all three branches

---

[85] Foreign Intelligence Surveillance Act of 1978 (FISA), 50 U.S.C. § 1801 et seq. (1978); USA PATRIOT Act of 2001, 107 Pub. L. No. 56, § 215, 115 Stat. 272, 287–88 (2001) (codified in scattered titles of U.S.C.).

[86] USA PATRIOT Improvement and Reauthorization Act of 2005, 120 Stat. 196 § 106 (codified as amended at 50 U.S.C. § 1861(b)(2)(A)).

[87] FISA § 1801.

[88] *Id.* at 64.

[89] United States v. United States District Court for the Eastern District of Michigan, 407 U.S. 297, 308 (1972).

of government.[90] FISA also created the Foreign Intelligence Surveillance Court ("FISC") to provide judicial oversight of the government's authority and to handle the classified information encompassed by foreign intelligence.[91] Under the original FISA, any governmental agency seeking to use electronic surveillance for *foreign intelligence* purposes must obtain a warrant by showing probable cause that the target is an agent of a foreign power.[92] Between its enactment in 1978 and September 11, 2001, FISA only slightly widened its scope to include methods of investigation beyond electronic surveillance.[93]

B. September 11, 2001, and the USA PATRIOT Act

The events that took place on September 11, 2001, caused the greatest number of casualties from a terrorist act on United States soil.[94] In response to the 9/11 attacks, Former President George W. Bush declared a "war on terrorism."[95] On October 4, 2001, the Senate proposed legislation designed to enhance law enforcement's ability to investigate potential and actual acts of terrorism.[96] The Senate passed the bill with a vote of 96-to-1 after ten days.[97] The House of Representatives proposed and approved its own version of an anti-terrorism bill the following day by a vote of 337 to 79.[98] These measures led to the USA PATRIOT Act of 2001, passed by Congress on October 25, 2001, and signed into law by President Bush the next day.[99] The USA PATRIOT Act

---

[90] PRESIDENT'S REVIEW GROUP REPORT, *supra* note 9, at 65.

[91] *Id.* at 66.

[92] 50 U.S.C. §§ 1801–11.

[93] PRESIDENT'S REVIEW GROUP REPORT, *supra* note 9, at 68.

[94] Jennifer C. Evans, *Hijacking Civil Liberties: The USA Patriot Act of 2001*, 33 LOY. U. CHI. L.J. 933, 959 (2002) [hereinafter *Hijacking Civil Liberties*].

[95] George W. Bush, Statement by the President in His Address to the Nation (Sept. 11, 2001), *available at* http://georgewbush-whitehouse.archives.gov/news/releases/2001/09/20010911-16.html.

[96] Evans, *supra* note 94, at 966.

[97] *Id.* at 966.

[98] *Id.* at 967.

[99] *Id.*

was designed to strengthen domestic security and broaden the powers of law enforcement agencies to identify and stop terrorism.[100] Split into ten parts, Title II: Enhanced Surveillance Procedures authorizes metadata collection under Section 215.[101]

C. The Metadata Collection Program is Created under Section 215 in Two FISC Orders

When FISA was originally enacted in 1978, the government did not have authority to compel documents.[102] Congress amended FISA in 1998 after the Oklahoma bombings to allow FISC to compel a narrow set of documents.[103] The USA PATRIOT Act significantly expanded FISC's authority to compel documents, but was narrowed in the USA PATRIOT Act Improvement and Reauthorization Act of 2005.[104] As codified, Section 215 authorizes FISC to issue an order for the "production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism."[105] Through two FISC orders, however, the systematic metadata collection program was created. First, FISC authorized mass collection of metadata in the "Primary Order."[106] Second, Verizon was ordered to submit metadata to FISC and the NSA on an ongoing basis through the "Secondary Order."[107]

---

[100] *Id.* at 965.

[101] USA PATRIOT ACT OF 2001, 107 PUB. L. NO. 56, § 215, 115 STAT. 272, 287–88 (2001) (CODIFIED IN SCATTERED TITLES OF U.S.C.).

[102] PRESIDENT'S REVIEW GROUP REPORT, *supra* note 9, at 80.

[103] *Id.*

[104] *Id.* at 81; USA PATRIOT Improvement and Reauthorization Act of 2005, 120 Stat. 196 § 106 (codified as amended at 50 U.S.C. § 1861(b)(2)(A)).

[105] USA PATRIOT ACT § 215.

[106] Primary Order, *supra* note 4.

[107] In re Application of the FBI for an Order Requiring the Prod. of Tangible Things From Verizon Bus. Network Servs., Inc. ex. rel. MCI Commc'n Servs. Inc. d/b/a Verizon Bus. Servs., No. BR 13–80, 2013 U.S. Dist. LEXIS 147002, (FISA Ct. Apr. 25, 2013) [hereinafter Secondary Order].

1. The Primary Order to Collect Metadata

The NSA, under Section 215, issued a Primary Order in 2006 that set out the framework and requirements for the mass collection of metadata.[108] The Primary Order required a high-ranking NSA official to determine if there is a reasonable articulable suspicion that the number being queried is associated with an international terrorist organization.[109] Currently, there are 22 designated agents who can authorize a query.[110] These agents may access the information without approval from a FISC court order.[111] The Government must seek authorization for Section 215 periodically from FISC, which it does typically every 90 days.[112]

Since 2006, different FISC judges have authorized the use of Section 215 35 times.[113] However, during the authorization process, FISC found on one occasion that the Government failed to comply with the minimization procedures.[114] In January 2009, the government reported that it used an "alert list" to search metadata that was not approved under the requisite reasonable articulable suspicion standard.[115] The FISC judge concluded that the government engaged in systematic noncompliance and ordered the NSA to seek FISC approval before conducting any inquiry for a probationary six-month period.[116]

Once an agent authorizes a query of a suspect, the agent enters the phone number with which the suspect is associated.[117] The phone number is the original identifier and is called a "seed."[118]

---

[108] *Id.* at 3–4.
[109] *Id.* at 5–7.
[110] *Id.*
[111] *Id.* at 9.
[112] *Id.*
[113] In Re Production of Tangible Things from [Undisclosed Service Provider], Docket Number BR 08–13 (Mar. 2, 2009) (authorizing Section 215 35 times from 2006 through October 2013).
[114] *Id.*
[115] *Id.*
[116] *Id.*; Klayman v. Obama, 957 F. Supp. 2d 1, 18 (stating the probationary period lasted only six months).
[117] *Klayman*, 957 F. Supp. 2d at 16.
[118] *Id.*

When a seed is queried, it is referred to as a "hop."[119] When the phone number is initially queried during the first hop, the NSA captures all metadata directly associated with that seed.[120] The NSA can then make a second hop, in which the NSA captures all metadata associated with each number identified from the first hop.[121] The NSA had authorization, until February 5, 2014, to make one additional hop, for a total of three hops.[122] Once the NSA has collected metadata from the three hops, it can conduct an unlimited number of searches with the breadth of data collected without oversight from FISC and without making additional reasonable articulable suspicion determinations.[123]

2. The Secondary Order Directing Verizon to Submit Metadata

The Secondary Order directed Verizon to provide to the NSA all metadata "on an ongoing daily basis."[124] It directed Verizon to produce "all call detail records" or "telephony metadata" created both between the United States and abroad, and "wholly within the United States, including local telephone calls."[125] The metadata included session-identifying information, trunk identifier, telephone calling card numbers, and call durations.[126] The last part of the order prohibited Verizon from disclosing any information given to the NSA or FBI.[127] Because of the gag order, Verizon and other phone companies could not discuss or reveal that their customers' metadata was being systematically transmitted to the NSA until the Snowden disclosures leaked the information.[128]

---

[119] ACLU v. Clapper, 959 F. Supp. 2d 724, 734 (S.D.N.Y. Dec. 27, 2013).
[120] *Id.*
[121] *Id.*
[122] *Id.*
[123] Klayman v. Obama, 957 F. Supp. 2d 1, 17.
[124] Secondary Order, *supra* note 107.
[125] *Id.* at 3.
[126] *Id.*
[127] *Id.* at 2–3.
[128] *Id.*

III. CURRENT CHALLENGES TO THE METADATA COLLECTION PROGRAM AUTHORIZED BY SECTION 215 OF THE USA PATRIOT ACT

Since Snowden revealed classified documents uncovering the metadata collection program, there have been several challenges regarding the constitutionality of Section 215. First, two U.S. District Courts have issued conflicting holdings regarding Section 215.[129] Second, the Presidential Review Group's massive review on the USA PATRIOT Act found Section 215 to be unconstitutional.[130] Third, none of President Obama's proposed changes to Section 215 have been passed into law.[131] Fourth, Congress proposed several pieces of legislation reforming Section 215 that are currently sitting in House Committees.[132]

A. Klayman v. Obama*: Section 215 is Likely to be Unconstitutional*

In *Klayman v. Obama*, the court found the NSA program "almost certainly" violates the Fourth Amendment.[133] The court distinguished the current NSA program from the pen register in *Smith*, claiming an "Orwellian" intelligence gathering system between telecommunication companies and the Government.[134] The court in *Klayman* found that the problem with this system is that people have entirely different relationships with phones today

---

[129] ACLU v. Clapper, 959 F. Supp. 2d 724, 757; Klayman v. Obama, 957 F. Supp. 2d 1, 43.

[130] PRESIDENT'S REVIEW GROUP REPORT, *supra* note 9.

[131] The White House, *FACT SHEET: The Administration's Proposal for Ending the Section 215 Bulk Telephony Metadata Program*, THE WHITE HOUSE (Mar. 27, 2014), http://www.whitehouse.gov/the-press-office/2014/03/27/fact-sheet-administration-s-proposal-ending-section-215-bulk-telephony-m [hereinafter *Obama's Proposal for Ending Section 215*].

[132] LIBERT-E Act, H.R. 2399, 113th Cong. (1st Sess. 2013); USA FREEDOM Act, H.R. 3361, 113th Cong. (1st Sess. 2013); Telephone Metadata Reform Act, H.R. 3875, 113th Cong. (2nd Sess. 2014).

[133] *Klayman*, 957 F. Supp. 2d at 32 ("I believe that bulk telephony metadata collection and analysis almost certainly does violate a reasonable expectation of privacy.").

[134] *Id.* at 33; *see supra* note 5 (defining "Orwellian").

than they did when the third-party doctrine was created in *Smith*.[135] Call records, which then would have given the police only scattered information about one's life, now "reveal an entire mosaic—a vibrant and constantly updating picture of the person's life."[136] The court further reasoned that modern society is better prepared and more willing to accept a reasonable expectation of privacy in a phone's metadata, making the metadata program unconstitutional under the Fourth Amendment.[137]

B. ACLU v. Clapper*: Section 215 is Constitutional under the Third-Party Doctrine*

In *ACLU v. Clapper*, the ACLU and other non-profit organizations filed a lawsuit less than a week after the disclosure of the Secondary Order.[138] The NSA collected metadata of the ACLU, a Verizon customer, as required by the Secondary Order.[139] The ACLU's phone records could be used to identify confidential clients such as journalists, legislators, and members of the public.[140] This, they argued, violated their First and Fourth Amendment rights.[141]

The court followed a strict reading of *Smith*.[142] It held that, because Verizon users—ACLU included—voluntarily transmitted numbers they dialed, there was no reasonable expectation of privacy in those numbers.[143] The court stated that the sheer volume of information the NSA can collect and store does not make it a Fourth Amendment violation.[144] Ultimately, the court dismissed the case for lack of standing. [145] The ACLU filed an appeal on

---

[135] *Klayman*, 957 F. Supp. 2d at 36.
[136] *Id.*
[137] *Id.*
[138] ACLU v. Clapper, 959 F. Supp. 2d 724, 735 (S.D.N.Y. 2013).
[139] *Id.* at 735.
[140] *Id.*
[141] *Id.*
[142] *Id.* at 751–52.
[143] *Id.* at 752.
[144] *Id.*
[145] *Id.* at 754.

March 6, 2014.[146] The Government's reply brief was filed on April 10, 2014.[147] The ACLU filed an additional reply brief on April 24, 2014, and the case is pending hearing as of the writing of this Article.[148]

C. The President's Review Group Report Recommends Terminating Metadata Collection due to Privacy Concerns

In response to the general concerns of the American public after the Snowden disclosures, President Obama created the Review Group on Intelligence and Communications Technologies ("President's Review Group").[149] The President's Review Group published a document ("The Report") consisting of 46 policy recommendations to the President that cover a variety of NSA programs, including Section 215 of The USA PATRIOT Act.[150] The recommendations consider both the public's civil liberties and the necessity of homeland security.[151] With respect to Section 215, The Report recommends the NSA end bulk storage of metadata.[152] It suggests a third-party hold the data instead.[153] The President's Review Group cites privacy concerns, similar to those discussed in this Article, as its justification for terminating the metadata program as currently administered by the NSA.[154]

---

[146] Brief for Plaintiffs-Appellants, ACLU v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. Dec. 27, 2013) (No. 14-42), https://www.aclu.org/sites/default/files/assets/corrected_brief_of_plaintiffs-appellants_-_final_stamped_03_07_2014.pdf.

[147] Brief for Defendants-Appellees, ACLU v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. Dec 27, 2013) (No. 14-42), https://www.aclu.org/sites/default/files/assets/2014-04-10_clapper_govt-opposition-brief.pdf.

[148] Reply Brief for Plaintiffs-Appellants, ACLU v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. Dec. 27, 2013) (No. 14-42) https://www.aclu.org/sites/default/files/assets/aclu_v._clapper_ca2_reply_brief_final_stamped.pdf.

[149] PRESIDENT'S REVIEW GROUP REPORT, *supra* note 9.

[150] *Id.*

[151] *Id.* at 1.

[152] *Id.* at 17.

[153] *Id.*

[154] *Id.* at 86–88 (citing In Re Production of Tangible Things from Undisclosed Service Provider, Docket Number BR: 08-13 (Mar. 2, 2009)).

D. President Obama's Proposed Changes and Pending Congressional Legislation

In a speech regarding the NSA's programs, President Obama told the American people that the metadata collection program would continue, although not as broadly.[155] However, through a Presidential Directive, President Obama eliminated the third hop.[156] Further, President Obama instructed the Attorney General to develop a new method to match the capabilities of Section 215 without the NSA actually holding the metadata.[157]

While several bills have been proposed to reform Section 215 in the House of Representatives, the USA FREEDOM Act has the most support with 142 co-sponsors.[158] The USA FREEDOM Act was introduced in the House of Representatives on October 29, 2013.[159] USA FREEDOM stands for "Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection, and Online Monitoring" Act.[160] This Act would amend the PATRIOT Act similarly to the LIBERT-E Act.[161] Both bills propose the FBI must include a statement of facts indicating that there are "reasonable grounds to believe that the tangible things sought are relevant and material to an authorized investigation" in order to request metadata records from a phone provider.[162]

On January 9, 2014, this bill was also referred to the subcommittee on Crime, Terrorism, Homeland Security, and

---

[155] President Barack Obama, Remarks by the President on Review of Signals Intelligence (Jan. 17, 2014) (transcript available at http://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence) [hereinafter President Obama's Remarks].

[156] *Id.*

[157] *Obama's Proposal for Ending Section 215*, *supra* note 131.

[158] USA FREEDOM Act, H.R. 3361, 113th Cong. (1st Sess. 2013); Congress, *Summary: H.R. 3361 – USA FREEDOM Act*, CONGRESS.GOV (Oct. 29, 2013), http://beta.congress.gov/bill/113th-congress/house-bill/3361; *see also* LIBERT-E Act, H.R. 2399, 113th Cong. (1st Sess. 2013); Telephone Metadata Reform Act, H.R. 3875, 113th Cong. (2nd Sess. 2014).

[159] *Summary: H.R. 3361 – USA FREEDOM Act*, *supra* note 158.

[160] *Id.*

[161] *Id.* at § 101(a)(1)(B).

[162] *Id.*

Investigations.[163] On May 22, 2014, this bill passed the House of Representatives as amended.[164]

IV. THE STANDARD TO SEARCH METADATA SHOULD BE RAISED TO A PROBABLE CAUSE STANDARD BECAUSE OF VAST PRIVACY CONCERNS

Benjamin Franklin once said, "Those who would give up essential Liberty, to purchase a little temporary safety, deserve neither Liberty nor Safety."[165] However, in the modern world, government surveillance of people at home and abroad is necessary to protect against threats that Mr. Franklin could never have imagined.[166] When does the government cross the line between safety and liberty? The Snowden leaks startled many Americans because of the seeming impossibility that a democratic state could become a surveillance state.[167] Civil liberties groups have called for the elimination of metadata collection—citing egregious civil rights violations—by bringing lawsuits against the NSA and President Obama.[168]

---

[163] *Id.*

[164] *Summary: H.R. 3361 – USA FREEDOM Act*, *supra* note 158.

[165] Benjamin Franklin, *Pennsylvania Assembly: Reply to the Governor, Nov. 11, 1755*, NATIONAL ARCHIVE FOUNDERS ONLINE, http://franklinpapers.org/franklin/framedVolumes.jsp?vol=6&page=238a (last visited July 31, 2014).

[166] In re FBI, No. 13-109, 2013 WL 5307991, at *30–31 (FISA Ct. Aug. 29, 2013) (stating that "telephony metadata" includes comprehensive communications routing information, such as including originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, International Mobile station Equipment Identity (IMEI) number, trunk identifier, telephone calling card numbers, and time and duration of call).

[167] *See supra* note 5 (defining "Orwellian").

[168] *E.g.*, ACLU, *Time to Rein in the Surveillance State*, ACLU.ORG, https://www.aclu.org/time-rein-surveillance-state-0 (last visited Apr. 25, 2014) ("The ACLU has been at the forefront of the struggle to rein in the surveillance superstructure, which strikes at the core of our rights to privacy, free speech, and association."); Electronic Frontier Foundation, *NSA Spying on Americans*, EFF.ORG, https://www.eff.org/nsa-spying ("EFF has been at the forefront of the effort to stop [surveillance of communications] and bring government surveillance programs back within the law and the Constitution.") (last visited Apr. 25, 2014).

Following public backlash regarding metadata collection, all three branches of the Government are taking action. After President Obama spoke to the American people specifically about Section 215 of the USA PATRIOT Act,[169] he issued a Presidential Policy Directive reigning in aspects of the metadata collection program. Additionally, there are roughly 30 different legislative bills before Congress altering the metadata collection program.[170] Two circuit courts have ruled on the opposite sides of the constitutionality of Section 215.[171] Political activist Larry Klayman appealed his case, *Klayman v. Obama*, directly to the Supreme Court on February 3, 2014, citing its "imperative public importance."[172] However, the Supreme Court denied his petition, leaving the constitutionality of Section 215 unresolved.[173] While the exact fate of the metadata collection program remains unknown, the Government's proposed actions merely provide a façade of change.

President Obama's Policy Directive and Congress' attempt at legislation with the USA FREEDOM Act are both superficial attempts at rectifying privacy concerns because the Government does not concede to the necessity of a warrant to search metadata, as required for searches under the Fourth Amendment. Instead, the current reasonable articulable suspicion standard is kept intact in the proposed legislation from both the House of Representatives and President Obama.[174] The Government, through FISC court documents, continually relies on the third-party doctrine in

---

[169] President Obama's Remarks, *supra* note 155.

[170] David Kravets, *Supreme Court passes on NSA bulk phone surveillance case*, ARS TECHNICA (Apr. 7, 2014, 6:46 AM), http://arstechnica.com/tech-policy/2014/04/supreme-court-passes-on-nsa-bulk-phone-surveillance-case/.

[171] Klayman v. Obama, 957 F. Supp. 2d 1, 43 (D.D.C. 2013); ACLU v. Clapper, 959 F. Supp. 2d 724, 757 (S.D.N.Y. 2013).

[172] 134 S. Ct. 1795 (Apr. 7, 2014).

[173] *Id.*

[174] *H.R. 3361 – USA FREEDOM Act*, *supra* note 158; President Obama's Remarks, *supra* note 155; Presidential Policy Directive/PPD-28, *Signals Intelligence Activities*, THE WHITE HOUSE (Jan. 17, 2014), www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

denying a reasonable expectation of privacy in metadata.[175] However, the third-party doctrine fails to take into account the vast privacy concerns associated with modern technology.

Because so much information about a person's private life can be gleaned from the collection of metadata, the Government should be required to obtain a warrant before searching metadata. As required by the Fourth Amendment, the standard for a warrant is probable cause.[176] Thus, the NSA should be required to make a probable cause determination to perform a "hop" on an American citizen's metadata. This requirement will protect citizens' privacy rights regardless of whether the NSA or the phone companies hold the metadata.

A. The Reasonable Articulable Suspicion Standard should be Updated because It Fails to Take Into Account the Reasonable Expectation of Privacy that should be Associated with Metadata

Although The President's Review Group found Section 215 to be unconstitutional, the metadata program may be a useful tool in the fight against terrorism, as President Obama has argued.[177] For this reason, instead of suggesting an end to the metadata program, the standard for searching metadata during a hop should be changed to require a higher burden of proof showing that the seed being queried is associated with terrorist activity. When FISA was originally enacted, the Government had to show probable cause to believe the target of the electronic surveillance was an agent of a foreign power.[178] This required FISC to obtain a warrant from a neutral and detached magistrate before accessing sensitive data.[179]

However, in the wake of 9/11, the threshold was lowered to require only "specific and articulable facts giving reason to believe

---

[175] *See, e.g.*, In re Application of the FBI for an Order Requiring the Production of Tangible Things from [Redacted], No. BR 13-109, 2013 WL 5741573 at *2–6 (Foreign Intel. Surv. Ct. Aug. 29, 2013).

[176] U.S. CONST. amend. IV.

[177] President Obama's Remarks, *supra* note 155.

[178] 50 U.S.C. § 1805.

[179] President's Review Group Report, *supra* note 9, at 88–89.

that the person to whom the records pertain is a foreign power or an agent of a foreign power."[180] This standard was too open-ended and Congress again changed the standard required to search metadata under Section 215 to "a statement of facts showing that there are reasonable grounds to believe that the tangible objects sought are relevant."[181] The standards used in both thresholds (the lowered one of 2001, and the slightly higher one of 2005) rely on the out-of-date third-party doctrine and privacy justifications.

Additionally, the Report points out the ease with which the NSA has abused the metadata program.[182] It cited that "[a]lmost 90 percent of the numbers on the alert list did *not* meet the 'reasonable, articulable suspicion' standard."[183] The NSA should be required to obtain a warrant from FISC before performing any queries because metadata reveals detailed information about a person.

1. Metadata Reveals Highly Personal and Sensitive Information Subject to Fourth Amendment Protection

Since the Snowden revelations, those in charge of intelligence have downplayed the significance of metadata.[184] President Obama assured the American people the content of calls was not being collected.[185] The Chairwoman of the Senate's Committee on Intelligence, Dianne Feinstein, remarked that "this is just

---

[180] *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. 107-56, § 215, 115 Stat. 272, 287 (2001) (codified as amended at 50 U.S.C. § 1861(a)(1)).

[181] USA PATRIOT Improvement and Reauthorization Act of 2005, 120 Stat. 196 § 106 (codified as amended at 50 U.S.C. § 1861(b)(2)(A)).

[182] President's Review Group Report, *supra* note 9, at 105.

[183] *Id.*

[184] *See, e.g.*, *Transcript: Diane Feinstein, Saxby Chambliss, Explain, Defend NSA Phone Records Program*, WASH. POST (Jun. 6, 2013), http://www.washingtonpost.com/blogs/post-politics/wp/2013/06/06/transcript-dianne-feinstein-saxby-chambliss-explain-defend-nsa-phone-records-program [hereinafter *Senator Feinstein's Remarks*]; President Obama's Remarks, *supra* note 155.

[185] President Obama's Remarks, *supra* note 155.

metadata."[186] Although voice content can be hard to process and difficult to collect on a mass scale, metadata is perfectly suited to computer analysis.[187] Metadata can show the context of a person's life and give an intimate look into one's interests, values, and societal roles.[188] Metadata can also be a rich source for obtaining sensitive information about one's identity, location, and social network.[189] When cross-checked against easily accessed public records, metadata can reveal a person's name, address, credit history, and more.[190] Although the metadata collection program offers powerful tools in the fight against terrorism, it severely implicates personal expectations of privacy.[191]

In an Amici Curiae Brief written in support of a reversal of *ACLU v. Clapper* by the Electronic Frontier Foundation, a small but compelling example is given demonstrating the sensitivities associated with the collection of metadata. If a single telephone call to a bookie is made, it suggests that a person likely made a bet.[192] But an analysis of metadata over time could reveal that the same person has a gambling problem.[193] While aggregating metadata is troubling for an individual, it is even more troubling when connections are made between individuals and larger social trends.[194] Analysis of metadata over time can "map the associations of individuals, revealing friendships, business

---

[186] Senator Feinstein's Remarks, *supra* note 184.

[187] Brian Lam, *Phew, NSA Is Just Collecting Metadata. (You Should Still Worry)*, WIRED.COM (June 19, 2013), http://www.wired.com/2013/06/phew-it-was-just-metadata-not-think-again/.

[188] *Id.*

[189] David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 64 (2013).

[190] Dan Roberts & Spencer Ackerman, *Anger Swells After NSA Phone Records Court Order Revelations*, THE GUARDIAN (June 6, 2013), http://www.theguardian.com/world/2013/jun/06/obama-administration-nsa-verizon-records.

[191] Grey, *supra* note 189, at 67.

[192] Brief for ACLU, et al. as Amici Curiae Brief of Experts in Computer and Data Science in Support of Appellants and Reversal, ACLU v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013) (No. 14-42) [hereinafter ACLU Amici Curiae Brief].

[193] *Id.* at 11–12.

[194] *Id.* at 12.

relationships, and social and political connections."[195] While this language focuses on the individual, collecting and searching metadata affects the lives of millions of Americans.

Each time the NSA performs a hop, the number of people Section 215 affects expands exponentially. For example, Person X is a suspect, and he made 100 phone calls. The NSA would have access to all 100 of those phone numbers Person X was in contact with. The NSA then has authorization to make a second hop; that is, to take the 100 phone numbers associated with Person X and look at the metadata associated with *each* of those numbers.[196] Further, if the 100 people Person X contacted each also contacted 100 people, the pool of metadata would now include 10,000 total phone numbers (100 people times 100 phone numbers).

A third hop would take the 10,000 phone numbers that were pooled during the second hop, and look at every number that was contacted. If each of those 10,000 people called 100 people, the metadata pool would now consist of 100 phone numbers (first hop) times 100 phone numbers (second hop) times 100 phone numbers (third hop), totaling a pool of one million phone numbers to query. Until President Obama's speech on January 17, 2014, the NSA had authorization to make the *third hop*.[197] FISC formally approved removing the third hop on February 5, 2014, stating its deletion adequately balances privacy and national security interests set forth in President Obama's Presidential Policy Directive.[198]

To illustrate this point with real people, an online blog, Webpolicy.org, performed a short-term study to learn if sensitive and personal inferences could be drawn from metadata.[199]

---

[195] *Id.*

[196] *Id.*

[197] *Id.*; President Obama's Remarks, *supra* note 155 ("Effective immediately, we will only pursue phone calls that are two steps removed from a number associated with a terrorist organization instead of the current three.").

[198] In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things, No. BR 14-01 (FISA Ct. Feb. 5, 2014); Presidential Policy Directive/PPD-28, *supra* note 174.

[199] Jonathan Mayer & Patrick Mutchler, *MetaPhone: The Sensitivity of Telephone Metadata*, WEBPOLICY.ORG (Mar. 12, 2014), http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata/ (last visited Apr. 28, 2014).

Beginning in November 2013, WebPolicy.org had participants install the "MetaPhone" application on their Android phones.[200] MetaPhone runs in the background of the user's device and submits device logs and social media information for analysis.[201] While this study is on a relatively small scale (546 participants), WebPolicy.org found that "phone metadata is unambiguously sensitive, even in a small population and over a short time window."[202] In total, the 546 participants contacted 33,688 unique phone numbers.[203] 18 percent of those numbers were identifiable by matching phone numbers against public records, such as Yelp and Google Places directories.[204] Participants had contacted Alcoholics Anonymous, labor unions, divorce lawyers, strip clubs, and sexually transmitted disease clinics.[205]

Additionally, the study indicated a pattern of calls that revealed more sensitive information than individual call records.[206] For example, a participant made phone calls to local neurology groups, a specialty pharmacy, a rare condition management service, and a hotline for a drug used solely to treat multiple sclerosis.[207] An inference can be made, based on this participant's metadata alone, that this participant has a serious medical condition. WebPolicy.org was able to corroborate this participant's medical condition proving that metadata does reveal personal and sensitive content.[208] Another participant had a long telephone call with her sister, then two days later placed a series of calls to Planned Parenthood.[209] She placed another series of calls two weeks later, and a final call a month after.[210] As this study shows, the NSA can gather and use power data with the tools it currently has at its disposal.

---

[200] *Id.*
[201] *Id.*
[202] *Id.*
[203] *Id.*
[204] *Id.*
[205] *Id.*
[206] *Id.*
[207] *Id.*
[208] *Id.*
[209] *Id.*
[210] *Id.*

To collect and search a person's metadata, the government should have to show probable cause that the person whose records are being searched is associated with international terrorism or clandestine intelligence activities.[211] Gathering the metadata on Person X and everyone whom each of those 100 people contacted is an egregious violation of privacy. Because of the privacy implications and the breadth of information that can be quickly amassed, the NSA should not be allowed to collect metadata without individualized suspicion that Person X is associated with terrorism.

2. The Third-Party Doctrine should be Updated in Light of Modern Technology

The third-party doctrine should be updated to reflect the modern relationship between a person and his cell phone. In *United States v. Jones*, Justice Sotomayor foreshadowed concerns over gathering information through surveillance, noting it could lead to "a too permeating police surveillance."[212] She suggested that it might be "necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[213] Much like Justice Brandeis' dissent in *Olmstead v. United States*, Justice Sotomayor's concurrence is at the forefront of the privacy argument in the new age.[214]

The third-party doctrine, as established in *Smith v. Maryland*, states that there is no reasonable expectation of privacy in information voluntarily handed over to a third-party.[215] FISC relies

---

[211] 50 U.S.C. § 1861(a)(1) (using the same language as the statute that the "tangible things sought are relevant . . . against international terrorism or clandestine intelligence activities").

[212] United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayer, J., concurring) (internal quotation marks omitted).

[213] *Id.* at 957.

[214] ACLU Amici Curiae Brief, *supra* note 192, at 11 (using Justice Sotomayor's concurrence to make the argument that aggregated metadata generated a comprehensive record of people's habits).

[215] Smith v. Maryland, 442 U.S. 735, 745 (holding there is no reasonable expectation of privacy when a person voluntarily gives their number to a third

on the holding in *Smith* to defend the production of metadata by telephone service providers to the NSA.[216] A person who gets a cell phone voluntarily discloses metadata to his or her cell carrier, a third-party, and his or her expectation of privacy is defeated. However, the facts of *Smith* are vastly different from what the NSA is doing under Section 215.[217] Today's circumstances have become so unlike those of the 1970s that the precedent set in *Smith* becomes completely frustrated. These circumstances include the Government's surveillance capabilities, the modern day relationship users have with their cell phones, and the relationship between the phone companies and the NSA.[218]

In *Klayman*, the Court found four main reasons that the third-party doctrine cannot justify the modern surveillance program under Section 215.[219] First, the pen register installed on Smith's phone was to last a mere 13 days, and it collected data regarding that case only.[220] Thus the information collected was short-term and highly limited.[221] In contrast, the information that the NSA collects is vast and on-going over the course of half a decade.[222] Second, in *Smith*, the police requested the phone company install the pen register on its own equipment to record the numbers dialed.[223] Under the current Secondary Order, telephone companies are required to provide the NSA records "*on a daily basis*."[224] The Government forces the third-parties (the telephone companies) to "create a formalized policy under which the service provider collects information for law enforcement purposes,"

---

party).

[216] In re FBI, No. 13-109, 2013 WL 5307991, at *9 (FISA Ct. Aug. 29, 2013).

[217] *See* Klayman v. Obama, 957 F. Supp. 2d 1, 32.

[218] *Id.*

[219] *Id.* at 32–34.

[220] *Id.*

[221] *Id.*

[222] *Id.* (noting the metadata program could last indefinitely so long as the war on terror persists, which could be forever versus the collection of information in *Smith* was specifically to convict Smith of one crime, to be used in one trial, and then discarded).

[223] *Id.* at 17.

[224] *Id.* at 19 (emphases added) (quoting Secondary Order, *supra* note 107)

circumventing the Fourth Amendment.[225]

Third, the *Smith* Court in the 1970s could not have conceived of the collection of metadata on such an expansive scale.[226] Finally, the scale on which people use their phones is inherently different than it was in the 1970s.[227] Not only is there a significant increase in phone usage (71,958,000 homes with phones in 1979 versus 326,475,248 mobile subscribers in 2012),[228] but the relationship between phone and user is also more personal than ever before.[229] Because of modern and intimate use of phones, information that is gleaned from metadata has changed not only in quantity but also in quality.[230]

Creating a trail of metadata is an unavoidable byproduct of modern life and metadata should not be considered in a vacuum.[231] The ACLU Amici Curiae Brief argued that metadata is generated through the "innumerable and near-continuous digital transactions and interactions" presented by modern life.[232] Financial transactions, medical records, travel records, communications, legal proceedings, biological information, education, health care, and entertainment are personal "digital tracks" every person leaves by simply participating in modern life.[233] Acts such as applying for a loan, renting a DVD, sending or receiving a package, files, or receiving medications through the mail generate metadata.[234] It would be practically impossible for an individual to avoid creating metadata in today's world.[235] A person can no longer assume the risk that their information may be handed over to a third-party because this transaction has now become a daily, if not hourly, occurrence.

Information that was once scattered now reveals a mosaic of a

---

[225] *Id.* at 19.
[226] *Id.*
[227] *See id.* at 20–21.
[228] *Id.* at 20.
[229] *See id.* at 20–21.
[230] *Id.*
[231] ACLU Amici Curiae Brief, *supra* note 192, at 15.
[232] *Id.* at 16.
[233] *Id.*
[234] *Id.* at 16–17.
[235] *Id.* at 18.

person's life.[236] The modern changes in technology render the third-party doctrine outdated and in need of a new jurisprudence that considers an updated look at the expectation of privacy in metadata information.

B. The Actions Proposed by the Government are Ineffective because They Maintain the Lower "Reasonable and Articulable Suspicion" Standard

The Government's proposed legislation is ineffective because it fails to raise the needed threshold to probable cause and continues to diminish citizens' privacy concerns. Representative James Sensenbrenner, Jr., the original author of the USA PATRIOT ACT and lead author on the proposed USA FREEDOM Act, acknowledged that "the NSA was doing some things that were far beyond what the intent of the law should have been . . . ."[237] He criticized Senator Feinstein's proposed legislation, specifically noting that her bill "is a joke" and her view is essentially that "if you like your NSA, you can keep it."[238] What Congress and the President fail to mention, however, is that the problem lies not only with mass collection of metadata, but also in the *way the Government is able to access and search* the metadata. This troubling standard remains unchanged and leaves the door open to a multitude of privacy violations.

President Obama's Policy Directive is superficial because it fails to provide any substantial changes that protect privacy rights. In President Obama's speech to the American people, he proudly claimed to end Section 215 metadata collection "as it currently exists."[239] However, bulk collection is not the biggest problem. The problem is not *where* the metadata is being stored, but *how* the

---

[236] Klayman v. Obama, 957 F. Supp. 2d 1, 36 (referencing the mosaic theory from Maynard, 615 F.3d at 562–63).

[237] Brendan Sasso & Bob Cusack, *Patriot Act author: Feinstein's bill 'a joke'*, THE HILL (Dec. 10, 2013, 6:00 AM), http://thehill.com/homenews/house/192561-feinsteins-nsa-bill-is-a-joke-says-rep-james-sensenbrenner.

[238] *Id.*

[239] President Obama's Remarks, *supra* note 155.

metadata is accessed.

First, President Obama limited the NSA to searching metadata within only two hops of the selection term being used instead of three.[240] Second, the metadata would no longer be collected in bulk by the NSA but would remain with the phone companies.[241] Third, the NSA would obtain the records pursuant to individual orders from FISC.[242] Although these recommendations appear to solve the problem of "dragnet surveillance," they fail to provide any real safety from abuse by the NSA.[243]

The problem with President Obama's Presidential Policy Directive is that it is not binding.[244] Presidential Directives can be amended or withdrawn at any time by the current President.[245] Even if Americans trust President Obama to follow through on the policy directives he proposed, the president in 2016 could reverse those changes with the swipe of a pen.[246] Unless codified in a statute by Congress, any future president, at any time and for any reason, could re-instate the third hop and bring metadata collection back under the purview of the NSA.

Additionally, none of the bills Congress has offered produce any substantial change to Section 215. None of the thirty-plus bills mention raising the standard from reasonable, articulable suspicion to probable cause. Most of the bills proposed, including the flagship USA FREEDOM Act, herald an ending to bulk metadata collection.[247] However, the USA FREEDOM Act barely amends

---

[240] *Obama's Proposal for Ending Section 215*, *supra* note 131.

[241] *Id.*

[242] *Id.*

[243] Electronic Frontier Foundation, *NSA Spying on Americans*, EFF.ORG, https://www.eff.org/nsa-spying (last visited Apr. 14, 2014) ("The US government, with assistance from major telecommunications carriers including AT&T, has engaged in a massive illegal dragnet surveillance of domestic communications and communications records of millions of ordinary Americans since at least 2001.").

[244] Todd F. Gaziano, *The Use and Abuse of Executive Orders and Other Presidential Directives*, THE HERITAGE FOUNDATION (Feb. 21, 2001), http://www.heritage.org/research/reports/2001/02/the-use-and-abuse-of-executive-orders-and-other-presidential-directives.

[245] *Id.*

[246] *Id.*

[247] *Summary: H.R. 3361 – USA FREEDOM Act*, *supra* note 158.

the current standard. Current law requires the government to submit a statement of facts showing reasonable grounds to believe that the tangible things or records sought are relevant to an authorized investigation.[248]

Yet Section 101 of the USA FREEDOM Act would require the Government to show that the tangible things sought are relevant and material to an authorized investigation and that they pertain to (a) a foreign power or an agent of a foreign power, (b) the activities of a suspected agent of a foreign power who is the subject of such an authorized investigation, or (c) an individual in contact with, or known to, a suspected agent of a foreign power who is the subject of such authorized investigation.[249] This proposed change only narrows what can be considered an "authorized investigation." The NSA would still be able to collect and search metadata based on the lowered standard of reasonable and articulable suspicion.

Unless the standard necessary to collect and search metadata is raised to probable cause and requires the NSA to obtain a search warrant from a neutral and detached magistrate, the same concerns that are currently present could be reinstated even if the proposed actions are implemented. FISC could reinstate dragnet bulk metadata collection under the NSA's direction. FISC previously concluded in 2009 that for two-and-a-half years the NSA had "frequently and systematically violated" the minimization procedures put in place to prevent abuse.[250] FISC Judge Walton also found additional noncompliance issues involving trained analysts querying the metadata without being aware that they were doing so.[251] The FBI could once again issue National Security Letters forcing Verizon and other telecommunication companies to comply with ongoing metadata disclosure. Verizon would have no way to disclose such an order to the public because every National Security Letter contains a gag order forbidding the receiver from

---

[248] USA PATRIOT Improvement and Reauthorization Act of 2005, 120 Stat. 196 § 106 (codified as amended at 50 U.S.C. § 1861(b)(2)(A)).

[249] *Summary: H.R. 3361 – USA FREEDOM Act*, *supra* note 158.

[250] President's Review Group Report, *supra* note 9, at 105.

[251] *Id.* at 106.

revealing the Letter's existence.[252] The actions the Government, including President Obama and Congress, are proposing are simply not enough to protect American citizens' privacy rights.

It is unlikely that searching metadata in the fight against terrorism will ever cease.[253] By requiring the standard to be raised to probable cause instead of reasonable and articulable suspicion, Americans will know their privacy is protected under the Fourth Amendment no matter what agency or company is holding their metadata.

CONCLUSION

The metadata information the Government is able to collect, store, and search on a massive scale makes Section 215 a violation of the Fourth Amendment. The Fourth Amendment is clear: to search a constitutionally protected area, one must have probable cause and obtain a warrant from a detached and neutral judge.[254] That is not being done under the metadata program.[255] Although the Government has proposed legislation to modify parts of Section 215, it has failed to change the standard under which the NSA can *search* metadata. Because enormous amounts of information can be gleaned from metadata revealing the intimacies of a person's life, it is time to recognize a right to privacy in metadata. By giving metadata *Katz*-level protection, metadata should be protected under the Fourth Amendment. This would require the NSA to seek a warrant from FISC showing probable cause that the suspect is linked to terrorist activity. Requiring a higher standard for the Government to perform any search of metadata adequately balances the need for privacy in this

---

[252] Electronic Frontier Foundation, *National Security Letters*, EFF.ORG, https://www.eff.org/issues/national-security-letters (last visited Apr. 28, 2014).

[253] David Kravets, *supra* note 170.

[254] *See* Katz v. United States, 389 U.S. 347, 357 (recognizing that the Fourth Amendment imposes a warrant requirement for searches and seizures because warrantless searches are unreasonable per se).

[255] USA PATRIOT Improvement and Reauthorization Act of 2005, 120 Stat. 196 § 106 (codified as amended at 50 U.S.C. § 1861(b)(2)(A)) (Section 215 does not show a requirement for a probable cause determination to be made and a warrant to be issued before searching the metadata).

enormous amount of sensitive information with the need to protect Americans from future terrorist threats.