Public Knowledge

July 7, 2016

Ms. Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

Re: CG RM-11771; WC Docket No. 16-143; WC Docket No. 05-25; WC RM-10593; WC Docket No. 16-106

Dear Ms. Dortch:

On August 29, 2016, Harold Feld, Senior V.P., Public Knowledge ("PK") met with Gigi Sohn of Chairman Wheeler's Office with regard to the above captioned proceedings.

DSCR (CG RM-11771)

Public Knowledge noted that the objections to the request for a "stay of operation" have confused a judicial stay (or stay of the operation of an FCC Order) with the request for an interim rule prohibiting operation. This is a Petition for Rulemaking. The 2004 Order establishing service rules for DSRC went into effect many years ago. Rather, Petitioners seek two things. An interim rule prohibiting operation (a "stay of operation") until resolution of final rules, and final rules consistent with the request in the Petition. *I.e.,* non-commercial use only, a cybersecurity plan and adequate privacy protections.

Accordingly, arguments referencing the *Virginia Jobbers* standard are utterly beside the point. The question is simply what serves the public interest, and whether an interim rule prohibiting operation of DSRC pending final modification of the rules is necessary in the public interest to protect the public from the enhanced risk of cyber attack and enhanced risk that DSRC licensees will capture and misuse personal information pending formulation of final rules.

PK does not propose that the Commission prevent providers from deploying equipment. Indeed, given that equipment is included in cars that may already be for sale, it would be impossible to prevent DSRC licensees from deploying. Rather, Petitioners seek an interim rule that would prevent licensees from activating the DSRC systems until the Commission can adopt final rules to protect the public. In addition to protecting the public from the dangers outlined in the Petition and initial comments, such an interim rule would make it clear that DSRC licensees must conform their systems to the final rule when adopted, and that systems deployed before adoption of the final rule will not be grandfathered.

PK also noted that DSRC licensees are already deploying at the risk that they will need to conform to whatever rule NHTSA adopts, assuming NHTSA adopts a mandate along the lines of the 2014 ANPRM. DSRC licensees that choose to deploy are therefore already acting under

considerable risk that they will need to reconfigure systems to NHTSA's final rule. Requiring them to wait to activate their "pre-standard" systems imposes no additional cost.

Non-Commercial Condition

PK noted that none of the DSRC licensees defended commercial use of DSRC spectrum. Nor did any DSRC licensee explain how commercial applications on DSRC spectrum using DSRC systems is consistent with the "privacy by design" features proposed by NHTSA. Nor did any licensee address how they intended to protect against cyber threats as a consequence of exposing cars, through DSRC spectrum, to mobile payment systems or other outside devices that may carry malware. [cite gas pump] The FBI, the DOT and the Federal Trade Commission have consistently warned consumers to be wary of connecting devices to cars. [cites] DSRC licensees appear willing to disregard these warnings and retain the freedom under the existing service rules to load and activate whatever commercial applications they wish.

Only a single party, CTIA, defended permitting DSRC licensees to exploit public safety spectrum commercially. As an initial matter, this is a somewhat astounding turn around for CTIA. In the Incentive Auction proceeding, for example, CTIA expressed considerable disapproval of permitting legacy licensees that did not obtain their spectrum at auction to enjoy spectrum windfalls. CTIA's newfound embrace of commercial applications for all users of spectrum – regardless of whether or not they obtain that spectrum at auction, or whether they compete directly against CTIA's members (as DSRC-enabled cars invariably will) – is highly noteworthy and a factor the Commission should consider in numerous pending and future spectrum proceedings.

Even CTIA, however, failed to provide any rationale for permitting DSRC licensees to exploit public safety spectrum commercially. If anything, CTIA's defense of commercial use – that commercial users are diligently working to address malware – underscores the danger of permitting unprotected commercial applications on DSRC systems. Consumers cannot tolerate "best efforts" on software that connects to automobiles capable of causing death to passengers and others if cyber hackers disrupt critical engine functions.

Therefore, if the Commission does not issue an interim rule prohibiting operation of DSRC systems in their entirety pending formulation of a final rule, the Commission should issue an interim rule prohibiting any commercial use of DSRC spectrum pending adoption of appropriate public safety rules. Again, ***not a single DSRC licensee defended commercial use of DSRC spectrum***, or even addressed it. DSRC licensees provided no plans for commercial applications, or explained why even a permanent non-commercial condition would in any way impact the deployment, safety or efficacy of DSRC's public safety purposes.

In the absence of any explanation of how a non-commercial rule would impact the DSRC licensees, let alone any defense of commercial use as necessary in the public interest, the Commission should – at a minimum – adopt an interim rule prohibiting commercial use of DSRC spectrum pending formulation of final privacy and cyber security rules.

WC Docket No. 16-143; WC Docket No. 05-25; WC RM-10593 (BDS)

PK recommended that the Commission should measure whether a BDS market is competitive using the standard metrics it employs in merger analysis: primarily HHI and overall market share, supplemented by any other relevant factors identified by the providers in the market, customers in the market, or the Commission on its own initiative.

To implement the new framework, the Commission should assume as an initial matter that all markets are non-competitive and that providers of BDS service bear the responsibility of filing an application demonstrating effective competition under the criteria adopted by the Commission. This is consistent both with the overall state of the record, which demonstrates pervasive market power, and with the basic principles of administrative efficiency. Where markets are obviously competitive, the Commission can grant petitions for effective competition relatively swiftly.

PK urged the Commission recognize the difference between the proposal that ILECs be declared *non-dominant* as opposed to a finding that markets are considered *non-competitive.* A finding of non-dominance simply means that ILECs will no longer be held to a unique standard based on their historic position in the market. This is different from the broader question of whether, in any given market, there are a sufficient number of carriers capable of providing the necessary vigorous competition to prevent charging customers monopoly rents.

WC Docket No. 16-106 (Broadband Privacy)

PK noted the Ninth Circuit's decision in *AT&T Mobility, LLC v. FTC*. PK urged the Commission to conclude the pending rulemaking as swiftly as possible to provide consumers with clear protections for their privacy in the provision of broadband service. PK also urged that the Commission clearly delineate its area of jurisdiction and the jurisdiction of the FTC, and to reaffirm that the agencies will continue to cooperate with each other to ensure that no gap in consumer protection exists for broadband access services and other online services.

The Commission should reject the proposed FTC more sensitive/less sensitive framework. PK reiterated previous arguments against adopted the proposed framework under which only "sensitive" information would require opt in consent, whereas opt out consent would be considered adequate for "less sensitive" information. While such a framework may be appropriate under Section 5 of the FTCA, which is designed as a general consumer protection statute, Section 222 provides both specific instructions with regard to the treatment of material, and must be read in the context of the broader Communications Act.

For example, the sensitive/non-sensitive dichotomy cannot apply to information Congress has already singled out as being unusually "sensitive" and expressly covered by Section 222(c) or Section 222(b). Because Congress has directed that such information be subject to specific safeguards, it would constitute "sensitive" information even if the FTC would not generally treat the information as "sensitive" under its own statutory framework.

Even if one assumed that the Commission should apply the "sensitive/non-sensitive" framework to Section 222(a) information, the Commission would still need to consider whether its privacy protections fit into the overall goals and purposes of the communications act. For example, if a provider can identify a device as belonging to a child (for example, as a consequence of parental blocking being enabled), sharing that information with advertisers would violate the spirit, if not the letter, of the FCC's restrictions on children's advertising.

Similarly, the FCC must take into account its traditional focus on encouraging diversity of views and information when evaluating whether information with regard to race or gender is "sensitive." To give an example, an advertiser for content services (movies, television shows, streaming media) may ask a BIAS provider to target individuals based on racial and gender stereotypes rather than established patterns of behavior. It is one thing for a sports network to advertise basketball to one person and hockey to another person based on a demonstrated pattern of behavior (e.g., streaming NHL.com or NBA.com). It is another thing for an advertiser to advertise basketball to someone identified by their zipcode as likely to be African American based on racial stereotypes about whether African Americans like basketball or hockey. The same is true with advertising movies featuring Latino lead actors primarily to those identified to the bias provider as Latino (for example, via a customer survey, guess based on last name, or address).

Rather than engage in such a complex analysis, the Commission should simply require opt in as the general requirement. In the absence of any evidence quantifying the supposed danger of "over exclusion" of information, the Commission should side with the clear Congressional purpose of favoring consumer control.

The Commission should not exempt "de-identified" data from the consent requirement. PK reiterated its previous opposition to exempting "anonymized" or "de-identified" information from the statute. The statute does not refer to any such exemption, and the Commission should not import such an exemption into the statute as contrary to the intent of Congress to give consumers control over their personal information.

As the Commission has already indicated in the *Notice*, even if one could read the statute as permitting anonymized data, several practical problems abound in preventing the exception from swallowing the rule and making the remaining protections of the statute useless.

(a) Anonymization must be meaningful or it is useless. It is not simply that any anonymized information can, in theory and with the expenditure of sufficient resources, be re-identified. Even assuming, that the market remains primarily focused on advertising, so that there is now no incentive for most entities, and discounting most extraordinary means of re-identifying data, it is difficult to see how a BIAS provider sharing "anonymized" information could prevent a third party from re-identifying the data.

(b) Contractual provisions would need to be dictated by the Commission – something providers have traditionally resisted. Assume a provider could make a showing that it has created a system that makes it sufficiently difficult to re-identify anonymized data. Technology changes, and third parties have access to data from other sources that may make it easier than anticipated to re-identify data. Alternatively, there may be

circumstances where third parties are willing to expend greater than usual resources to re-identify data (e.g., detective agencies, services doing opposition research on rival political parties. Foreign governments attempting to monitor expatriate citizens). To prevent re-identification, the Commission would need to mandate contractual terms prohibiting third parties from attempting to re-identify data, and hold BIAS providers accountable for failure to enforce.

(c) How could customers prove that BIAS providers were abiding by the agreements? Under the Cable Privacy Act, a customer is entitled to demand a written record of what information the cable operator collects and with whom the information is shared. This allows customers to trace a potential "leak" of personal data back to the cable operator. Section 222 does not provide an analogous provision for customers to "audit" the personal information collected by the network operator and its sharing practices. Without such a protection, it is impossible for any consumer to determine if the broadband provider is honoring the whatever regulatory or contractual protections the Commission might impose.

(d) The market continues to evolve, requiring constant vigilance. When the Commission adopted its initial voice CPNI rules, it did not anticipate the rise of pretexting, requiring modification of the rules only a few short years after adoption of the initial rules. Any rules adopted based on today's marketplace and technology would require constant monitoring and adjustment as the cost of re-identifying data decreases and demand for re-identified data emerges in response to availability. The Commission would need to constantly monitor the market place to ensure that the protections imposed to prevent de-identification today do not become meaningless.

In accordance with Section 1.1206(b) of the Commission's rules, this letter is being filed with your office. If you have any further questions, please contact me at (202) 861-0020.

Respectfully submitted,

/s/ Harold Feld
Harold Feld
Senior V.P.
Public Knowledge
1818 N Street, NW
Washington, DC 20036

Cc: Gigi Sohn