

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of)
) ET Docket No. 14-143
Mobile Device Theft Prevention)

COMMENTS OF MICROSOFT CORPORATION

Table of Contents

I.	Microsoft Is Committed to Enhancing the Safety of Its Smartphone Users	2
II.	A Federal Framework Is Preferable to State-by-State Regulation To Best Promote Engineering Innovation and Flexibility and Ultimately Deliver the Best Theft Deterrent Solutions to Smartphone Users	4
III.	Lock/Wipe/Restore Functionalities Require Linking an Authorized User to a Smartphone Before They Can Be Operational and Therefore the Features Cannot Be Operational "By Default"	7
IV.	Ongoing Study of Strengthening Smartphone Identifiers Should Be Undertaken on an Industry-Wide and Standards-Driven Basis.....	10
V.	Law Enforcement Agencies Should Increase Utilization of Existing Stolen Phone Databases	12
VI.	Improved Data Will Increase the Effectiveness of Smartphone Theft Deterrent Efforts by Industry, Law Enforcement, and Governments	14
VII.	Conclusion.....	18

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

In the Matter of)
) ET Docket No. 14-143
Mobile Device Theft Prevention)

COMMENTS OF MICROSOFT CORPORATION

Microsoft,¹ as a mobile operating system developer and a manufacturer of smartphones, is grateful to have had the opportunity to contribute its technological expertise to the Technological Advisory Council Subcommittee on Mobile Device Theft Prevention (“MDTP TAC”) and commends the Commission for directing an in-depth and data-driven investigation into the measures that could be taken to deter and reduce smartphone theft. Microsoft offers the following recommendations in response to the Public Notice:

- Smartphone theft deterrence measures should employ a multi-pronged approach that includes technology, consumer education, changes in consumer behavior, and effective law enforcement.
- Given voluntary industry initiatives, Microsoft does not believe regulation is needed in this area, but it would greatly prefer a federal framework addressing smartphone theft that reflects the voluntary industry commitments and

¹ Microsoft Corporation submits these comments in response to the *Public Notice* issued by the Office of Engineering Technology (“OET”) and the Consumer and Governmental Affairs Bureau (“CGA”) and the Wireless Telecommunications Bureau (“WTB”) of the Federal Communications Commission (“FCC” or “Commission”), collectively “Bureaus,” in the above-referenced proceeding. *Comments Sought on Technological Advisory Council Report on Mobile Device Theft Prevention*, Public Notice, ET Docket No. 14-143, DA 14-1828 (rel. Dec. 12, 2014) (“Public Notice”).

preempts state laws rather than a patchwork of varying state laws. The adoption of varying State “kill switch” laws is not only unnecessary because of industry commitments to implement theft deterrent features nationwide and two state laws that will have the effect of a nationwide implementation, but it also will be harmful to consumers due to the increased cost and complexity of trying to comply with multiple, differing state-by-state requirements. Further, additional state laws would limit engineering innovation and flexibility to the detriment of smartphone users.

- Microsoft would support a recommendation for implementing “lock/wipe/restore” functionalities on smartphones, as is evident by its participation in the CTIA Smartphone Anti-Theft Voluntary Commitment. However, the Commission should recognize that these functionalities depend upon having an authorized user, and therefore cannot exist “by default.”
- The MDTP TAC Report limited itself to consideration of smartphone theft and smartphone technologies and the Commission should, as requested by the Report, consider all recommendations within the scope of smartphones only.
- The most effective way to accomplish global scale for measures to strengthen smartphone identifiers would be to study and implement recommendations through technical standards bodies.
- Increased law enforcement subscription to and use of smartphone identifier databases developed and operated by wireless carriers would increase the utility of those databases as a law enforcement tool.
- Compiling better data and precise interpretation of that data will help industry, law enforcement, and governments get smarter and be more effective in battling smartphone theft.

I. Microsoft Is Committed to Enhancing the Safety of Its Smartphone Users

Microsoft shares the interests of policymakers in enhancing the safety of smartphone users. Microsoft’s CEO Satya Nadella consistently emphasizes that Microsoft is a cloud-first, mobile-first company. We have a strong interest in ensuring that everybody can use their smartphone with more confidence, that they feel comfortable doing so, and that they’re safe doing so. That’s the philosophy that’s

driving our enhancement of theft deterrent technology in Windows Phone smartphones.

In fact, Microsoft has long partnered with stakeholders on matters of public safety. Innovation is at the heart of Microsoft as a company, not just in how we make products but also in how we help to fight crime. For example, just over a year ago, Microsoft unveiled at its Redmond campus headquarters the Microsoft Cybercrime Center, a state-of-the-art secured facility housing groundbreaking Microsoft technologies that allow the team to visualize and identify global cyberthreats developing in real time, including SitePrint, which allows the mapping of online organized crime networks; PhotoDNA, a leading anti-child-pornography technology; cyberforensics, a new investigative capability that detects global cybercrime, including online fraud and identity theft; and cyberthreat intelligence from Microsoft's botnet takedown operations.

Closer to the subject at hand, Microsoft has offered remote lock and remote wipe features for over six years – the first smartphone to make those features available – and voluntarily committed to enhance those security features with functionality that can render a device inoperable in the event of theft and that will persist across attempts by unauthorized users to reset or flash the smartphone operating system. Those new features will be available on all Windows Phone smartphones in the United States manufactured after July 1st of this year.

II. A Federal Framework Is Preferable to State-by-State Regulation To Best Promote Engineering Innovation and Flexibility and Ultimately Deliver the Best Theft Deterrent Solutions to Smartphone Users

Microsoft understands the interest of state legislators around the country in deterring smartphone theft and is proud to deliver the technology to do so.

Notwithstanding the best of intentions of state legislators, however, additional state legislation governing theft deterrent technologies in smartphones threatens to reduce innovation and weaken the protections we otherwise are capable of developing. Two states – Minnesota and California – have implemented laws governing smartphone theft deterrent technology. Already in the month since the start of the 2015 state legislative session, 12 additional smartphone “kill switch” bills have been introduced in the states, and there are apt to be more.

These bills differ from another: some more prescriptive than others and each imposing slightly different requirements. Some bills include requirements that would not be technologically feasible such as the “active at purchase/default on” approach described below. Others specify the smartphone initial setup process or contain requirements that would, inadvertently, prevent the development and use of secure reverse logistics that the MDTP TAC Report recommends.² They cover different types of devices and some could require recalls of entire product lines that are already on store shelves. Some bills seek to micro-manage the technology and, if enacted, would restrict

² MDTP TAC Report at 73, § 8.3, Recommendation 3.2.

some of the innovative next generation anti-theft enhancements that Microsoft already is developing – enhancements that would be good for consumers and public safety but, because they fall outside of the existing vision of state legislators, could be inadvertently barred. One bill would even allow activation of consumers’ “kill switches” by the government to interrupt communications services including, in some instances, without a court order.

Mutual inconsistency among state theft deterrent requirements, which would require multiple versions of operating systems from state-to-state, would obviously be problematic and, most likely, unenforceable. The potential for conflicting state requirements is not the only problem, though: the continual addition of requirements state-by-state – even if they don’t conflict with one another – also is harmful to implementing powerful theft deterrent technology. In order to provide maximum security, Microsoft’s theft deterrent solution is very complex. These features involve contributions from and collaboration among many different engineering teams within the company. One feature interacts with and affects another. The addition of one new feature or requirement by one state’s law can require revisiting and reworking all the other features. The solid engineering, design, and testing takes time, and new state requirements often divert resources away from more effective innovations and improvements. The threat of new prescriptive state requirements also operates as a disincentive for developing and innovating because with the enactment of a single

state's new law, months of collaborative work by multiple teams on a new feature can be nullified and wasted.

State "kill switch" laws also are unnecessary. The industry already committed voluntarily to implementing theft deterrent technology in smartphones nationwide by July 2015.³ In addition, Minnesota and California have made smartphone theft deterrent technology a legal requirement. Because manufacturers do not produce smartphones on a state-specific basis, the Minnesota and California laws will, in practice, govern the features on smartphones nationwide.

Industry-wide theft deterrent commitments render regulation unnecessary. However, Microsoft strongly prefers a federal framework, reflective of the voluntary industry commitments, over the rolling imposition of varying state-by-state requirements given the harmful impact that the latter could have on theft deterrence and technology innovation. In the interest of promoting the safety of life and property through the use of radio communication, the Commission should act quickly to create a federal framework substantively reflective of the industry's Smartphone Anti-Theft Voluntary Commitment that preempts state legislation of smartphone theft deterrent technology.

³ See the CTIA Smartphone Anti-Theft Voluntary Commitment, *available at* <http://www.ctia.org/policy-initiatives/voluntary-guidelines/smartphone-anti-theft-voluntary-commitment>.

III. Lock/Wipe/Restore Functionalities Require Linking an Authorized User to a Smartphone Before They Can Be Operational and Therefore the Features Cannot Be Operational “By Default”

The Public Notice seeks comment on a recommendation for “making ‘lock/wipe/restore’ functionality operational by default on all mobile wireless devices.”⁴ Microsoft is pleased to report that smartphones running the Windows Phone operating system currently have lock/wipe/restore functionality through a free feature called “Find My Phone.” The Find My Phone website⁵ allows a user to locate the phone, cause it to ring (a useful feature if, for example, the phone has fallen behind a couch cushion), lock the phone remotely, leave a custom message on the lock screen (*e.g.* “If you have found this phone, please e-mail me at”) and wipe user data from the phone. In order to perform these actions, the phone must be powered on and the website must be able to connect to the phone through some form of network connectivity, such as cellular, cellular data, or Wi-Fi.

There has been within the states a fair amount of debate about theft deterrent features being operational “by default.” Theft deterrent features rely on providing access to authorized users and denying access to unauthorized users. The identity of the authorized user cannot exist in the operating system “by default” since a particular smartphone must, after purchase, be linked with the identity of the intended user. Thus,

⁴ Public Notice at 1.

⁵ The Find My Phone web portal is available at <https://www.windowsphone.com/en-us/my/find>.

until the authorized user links their identity to the device, the phone cannot have an “authorized user.” Because theft deterrent features depend upon the concept of an authorized user and because an authorized user cannot exist “by default,” the operation of lock/wipe/restore features also cannot be operational “by default.”⁶

Using Windows Phone as an example, the Find My Phone features cannot be operational “by default” because two user actions must occur. First, the user must have connected the phone to the user’s Microsoft Account user name and password. When the phone is first removed from its box after purchase, the phone is not connected to a particular user. It is only by registering a Microsoft account user name and password that the user can “tell” the phone that it has an authorized user and identify who that user is. Second, in order to operate any of the locate/ring/lock/screen message/wipe features, the user must visit the secure Find My Phone web portal, enter their Microsoft Account credentials, and instruct the feature to perform the desired task. Thus, while the feature is present on all smartphones sold in the United States running the Windows

⁶ The Report erroneously states that Minnesota and California laws require anti-theft functionality to be enabled “by default.” MDTP TAC Report at 32, § 3.5.11. To the contrary, the Minnesota law requires devices to come equipped with preloaded antitheft functionality *or be capable of downloading that functionality*; it says nothing about default options. The law’s downloadable option precludes a requirement of default enablement of anti-theft functionality. Likewise, the California law requires the smartphone “during the initial device setup process [to] prompt an authorized user to enable the technological solution.” The language contemplates that the device is *not* enabled until the user does something and, thus, anti-theft functionality is not on by default.

Phone operating system, it is not operational unless and until the authorized user performs some actions.

Microsoft understands the interest in increasing the likelihood of, or reducing barriers to, activation of theft-deterrent features. A constructive recommendation to industry could be to encourage consumer activation of theft deterrent features as early in the smartphone setup process as is reasonable. Alternatively, any recommendation using the term “by default” could clarify that the term means “activated upon association of an authorized user’s identification credentials with the smartphone, unless the user takes steps to disable the feature.”

The Public Notice question also refers to a recommendation in the MDTP TAC Report relating to providing lock/wipe/restore capabilities. Microsoft is not aware of such a recommendation within the Report and, if there were, the recommendation for making those features available would be counterintuitive given their universal availability⁷ and, as explained above, the technical limitations on default operability.

In addition, the Public Notice underlines the term “all mobile devices” in its question about making these functionalities operable by default. It should be emphasized that the Report restricted its scope to smartphones,⁸ thus the Report

⁷ MDTP TAC Report at 40 (“While specific behaviors may vary slightly, all solutions (except Qualcomm) provide these basic features: locate . . . ring . . . lock with PIN . . . erase . . . [and] web interface.”).

⁸ *Id.* at 9 (“The scope of this report has purposefully been limited to the theft of smartphones since smartphones are by far the largest component of the problem and is

cannot reasonably be interpreted as recommending lock/wipe/restore capabilities for mobile devices other than smartphones. If the underline in the Public Notice is intended to extend the scope of the question beyond smartphones, it has mischaracterized any implicit or explicit recommendation within the Report. The issue of whether, and how, to require such features on mobile devices other than smartphones is technologically complex and data is lacking to suggest such a requirement is needed. Given that these highly technical and complex issues have not been considered by the expert committee, Microsoft strongly urges the Commission to maintain the Report's scope of focus.

IV. Ongoing Study of Strengthening Smartphone Identifiers Should Be Undertaken on an Industry-Wide and Standards-Driven Basis

The Report does not have data to identify the international destinations for stolen smartphones,⁹ but it does note that sophisticated phone theft rings "are known to exist,"¹⁰ "some portion of phones are shipped overseas,"¹¹ and "[stolen p]hones *may*

sufficient[ly] complex as a topic of focus. Any references to mobile devices, mobile phones, [or] cellular phones in this report can be considered to be a reference to smartphones.").

⁹ MDTP TAC Report at 6 ("[T]he Mobile Device Theft Working Group was unable to obtain any definitive information on the destination of the millions of stolen smartphones. Anecdotal information seems to strongly suggest that at least a subset of the stolen smartphones are being exported from the United States to countries that are both geographically and politically remote from the U.S."); *see also id.* at 44, § 5.6 ("There is a lack of information about the number of smartphones that are shipped overseas." and "There is a lack of device trail of the stolen smartphones shipped overseas.").

¹⁰ *Id.* at 22, § 3.2.2.1.

¹¹ *Id.*

be packaged for shipment and use overseas.”¹² The Report also speculates that “[organized] criminals *may have* more sophisticated attack methods, for example changing the device identifier.”¹³ Solid data on these speculations would be useful in identifying the existence, size, and scope of international smartphone theft rings and their ability to modify smartphone identifiers. A data-driven understanding of the problem will help to prioritize smartphone identifier strengthening efforts.

The Report’s recommendation on this point was appropriate: rather than recommending enhancements to smartphone identifiers, it encouraged further study by the TAC MDTP Working Group into making identifiers more resistant to change if, after study, such a strengthening is deemed to be required.¹⁴ If identifier strengthening is something that, after study, is recommended, such efforts should have a global scale in order to be most effective. The best way to accomplish global scale for measures to strengthen smartphone identifiers would be to study and implement recommendations through technical standards bodies. Solutions that are ad hoc or are not driven by technical understanding will not be as effective as they could be in achieving their goal. Further, any solution that is not adopted for global application will leave open a country

¹² MDTP TAC Report at 19, § 3.1.3 (emphasis supplied).

¹³ *Id.* (emphasis supplied).

¹⁴ *Id.* at 74, §8.4, Recommendation 4.3 (explaining that the MDTP Working Group’s ongoing study should include an “examination of the usage of identifiers and making them more resistant to change by outside parties, if required.”).

or region where the solution is not utilized. If international phone theft rings do, in fact, exist widely and if they do, in fact, counterfeit smartphone identifiers, they would be likely to locate in regions that have not adopted the identifier strengthening technologies. Study and recommendations by an international standards body is the most promising method for avoiding those potential weaknesses.

V. Law Enforcement Agencies Should Increase Utilization of Existing Stolen Phone Databases

The stolen phone databases that mobile operators voluntarily established and operate are a helpful resource for information about the status of a particular smartphone. The databases, to which law enforcement agencies may subscribe for free, allow law enforcement agencies to ascertain whether a mobile operator has listed a particular smartphone as stolen. Mobile operators are the appropriate managers of the databases,¹⁵ but increased law enforcement subscription to the databases,¹⁶ including

¹⁵ See *MDTP TAC Report* at 44, § 5.1 (Not all device theft is reported to law enforcement. In many cases, customers make the report only to the carrier.”).

¹⁶ Microsoft understands there to be a low rate of subscription to the databases by law enforcement agencies, an understanding that is confirmed in the Report: “The industry’s database . . . is not widely used or known about especially by law enforcement.” *Id.* at 6. The lack of law enforcement utilization of this powerful tool in deterring smartphone theft may be due to the Report’s observation that “law enforcement officers may not be aware of the significance of the device identifier” and that “law enforcement officers are not fully aware of how to access information that is in the GSMA IMEI Database.” See *id.* at 44, § 5.1. Accordingly, Microsoft supports providing education to law enforcement on the significance of device identifiers and the usefulness of the databases.

more input to those databases on behalf of law enforcement about stolen (or found) phones, would increase the utility of the databases as a law enforcement tool.

More generally, many government officials have emphasized the need to reduce smartphone theft. The mobile industry (including OS providers, manufacturers, and mobile operators) has educated consumers and law enforcement agencies, developed and operates free smartphone identifier databases, created free technologies for remote smartphone control, and have created and are providing, at no charge, “kill switch” technology in newly manufactured smartphones. The development and provision of all the foregoing tools for law enforcement and consumers was performed voluntarily by and at the sole expense of the wireless operating system developers, manufacturers, and mobile operators.

Yet, truly effective theft deterrence requires a multi-pronged approach, of which technology is just a component. In addition to technology, this multi-pronged approach should include consumer education, changes in consumer behavior, and effective law enforcement. Available reports make it clear, in fact, that when law enforcement agencies focus their resources on preventing smartphone theft, they are remarkably effective.¹⁷ Therefore, law enforcement agencies be encouraged to direct

¹⁷ See, e.g., Jerold Chinn, “Muni Smartphone Thefts Plunge 77 Percent,” [SFBay](#) (May 13, 2014) (In 2013, San Francisco Municipal Transit Authority, using a federal grant, increased police presence on buses, trains, and cable cars, and began an “Eyes Up, Phone Down” campaign encouraging riders to pay attention to their surroundings, and fare inspectors passed out cards to riders on how to protect their smartphones.

resources to the effort, including free participation in carrier-developed and carrier-managed identifier databases, consumer education, patrols, and smartphone theft follow-up investigations.

VI. Improved Data Will Increase the Effectiveness of Smartphone Theft Deterrent Efforts by Industry, Law Enforcement, and Governments

Microsoft firmly believes in the need for improved empirical data gathering relating to smartphone theft. Better data will help industry, law enforcement, and governments get smarter and be more effective in their battle against smartphone theft. Quantifying smartphone theft, understanding where and when most smartphone thefts occur, evaluating the effectiveness of the variety of deterrent efforts (alone and in combination), and understanding the destination of stolen phones will provide better insight into the elements of smartphone theft, including the size and scope of the problem. This understanding, in turn, will help in evaluating whether it would be helpful to modify the relative importance being placed on the various components of anti-theft efforts.

Smartphone theft declined by 77 percent in that year.), *available at*: <http://sfbay.ca/2014/05/13/muni-smartphone-thefts-plunge-77-percent/>. *See also* "Reducing Mobile Phone Theft and Improving Security," UK Home Office at 16 (September 2014) (describing "Operation Ringtone," which targeted theft hotspots in London with increased patrols and sharing intelligence among law enforcement about mobile phone crime gangs), *available at* https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/390901/HO_Mobile_theft_paper_Dec_14_WEB.PDF; *see also id.* at 15 (targeted law enforcement efforts coinciding with the reduction in smartphone "theft-from-the-person" events).

Good data can reduce wasted efforts or undertakings of limited benefit, allowing resources of law enforcement and industry to be re-directed in a manner that is results-driven and more effective. Just as doctors prefer to understand an underlying medical condition before treating symptoms, we should not simply throw resources at deterring smartphone theft without further understanding its causes and motivations, its frequency, and its scope. With that understanding, the approach to deter smartphone theft will be informed and, likely, more effective.

The MDTP TAC did an excellent job assessing and explaining the issues and solutions, and delivering recommendations for the future, but it was forced to do so without the availability of credible, law enforcement-originated data:

- The Report highlights that “there are no current official national or international smartphone theft statistics.”¹⁸ It includes “preliminary” data from only 21 of roughly 18,000 law enforcement agencies (covering only 16 percent of the U.S. population)¹⁹ and concludes that “there is insufficient data to determine the extent and trend of criminal activity.”²⁰
- There is no data beyond anecdotal information to determine whether there are international phone theft rings, the size of the international market for stolen phones, and the destination of stolen phones.²¹ The definitive statement that “smartphone theft is an international issue” relies on anecdote.

¹⁸ MDTP TAC Report at 6.

¹⁹ *Id.*

²⁰ *Id.* (“The more troubling issue at this point is that it [is] challenging to obtain and analyze the data; thus there is insufficient data to determine the extent and trend of criminal activity.”).

²¹ *Id.* (“[T]he Mobile Device Theft Working Group was unable to obtain any definitive information on the destination of the millions of stolen smartphones. Anecdotal information seems to strongly suggest that at least a subset of the stolen smartphones

Better data is needed and Microsoft strongly supports the MDTP TAC Report's recommendation for collecting such data.²²

The data should be credible, relevant, and analyzed with precision. Microsoft is concerned that some of the "data" contained in the Report lacked credibility or was simply not relevant.

- The Report refers to a Consumer Reports consumer survey as a "dataset regarding crime."²³ The Consumer Reports consumer survey, however, asked questions intended to facilitate the magazine's *prediction* of whether the magazine thought smartphone theft might increase.²⁴ That prediction, moreover, was for the *previous* year (predicting the past) and was compared with the prediction for the previous year. Prediction 1 was compared to prediction 2 to make a prediction in 2014 about whether smartphone theft grew from 2012 to 2013. A magazine's prediction of that nature is of little empirical value, does not qualify as a "dataset" to define the scope of a problem,²⁵ and is inappropriate as the basis for government decision-making or serious anti-theft efforts.

are being exported from the United States to countries that are both geographically and politically remote from the U.S.").

²² MDTP TAC Report at 74, § 8.4, Recommendations 4.1 and 4.2; *see also id.* at 21, § 3.2.2.

²³ *Id.* at 21, § 3.2.2.

²⁴ *See* "Smart phone thefts rose to 3.1 million last year, Consumer Reports Finds," *Consumer Reports* (May 21, 2014) ("About 3.1 million American consumers were victims of smart phone theft in 2013, *Consumer Reports projects*, based on our latest nationally representative survey of adult Internet users. That's nearly *double the number we previously projected* had been stolen during 2012. The survey also projects that 1.4 million smart phones were lost and never recovered last year."), *available at* <http://www.consumerreports.org/cro/news/2014/04/smart-phone-thefts-rose-to-3-1-million-last-year/index.htm>. The article does not supply information about sample size of the survey or specific questions asked.

²⁵ It is little wonder, then, that the MDTP TAC Report found confusing the differential between actual and relatively recent data from law enforcement, on the one hand, and civilian predictions in a magazine on the other. *See* MDTP TAC Report at 23 ("The MDTP

- The Report references theft and robbery data from 2012 and 2013 that have no subcategory for smartphones.²⁶ If this data were relied upon as an indicator of smartphone theft, an increase in pickpocketing wallets would be misinterpreted as a rise in smartphone theft. Smartphone theft may be growing or declining at rates different than theft and robbery generally. Accordingly, statistics on theft and robbery generally are of little help in identifying trends in smartphone theft.

Better data will generate more effective allocation of resources to smartphone theft deterrence as long as interpretation of the data is precise and the data itself is relevant and credible.

Working Group was not able to confirm why phone thefts reported to law enforcement is [sic] much less than that estimated by Consumer Reports.”).

²⁶ The Report also concludes that “[c]ollected law enforcement data combined with FBI crime data would estimate that for 2013 one tenth of all thefts and robberies committed in the U.S. is associated the theft of a mobile phone.” MDTP TAC Report at 22, § 3.2.2. Empirical support for this conclusion, however, was not included.

VII. Conclusion

Microsoft looks forward to continuing to assist the Commission and the MDTP TAC in the data-driven study of smartphone theft and developing technological solutions to combat it.

Respectfully submitted,

MICROSOFT CORPORATION

/s/ Paula Boyd

Paula Boyd
Director, Government and Regulatory Affairs
901 K Street, NW, 11th Floor
Washington, DC 20001
202.263.5946
Paula.Boyd@microsoft.com

Gunnar Halley
Senior Attorney, Regulatory Affairs
One Microsoft Way
Redmond, WA 98052
425.703.3641
gunnarh@microsoft.com

30 January 2015