Submission from Apple Inc. and Apple Distribution International Limited on Revised Notices Regimes in the Investigatory Powers Act

Apple Inc. and Apple Distribution International Limited appreciate the opportunity to submit public comments on the Home Office's proposed reforms to the Investigatory Powers Act (IPA).

The IPA, passed in 2016, already grants the UK government extraordinary powers. For example, the IPA provides the government with, among other things, authority to issue secret orders requiring providers to break encryption by inserting backdoors into their software products. At the time, we objected to passage of the IPA, including its purported extraterritorial application. *See* Statement of Apple on Investigatory Powers Bill (Dec. 21, 2015). Apple similarly objects to the Home Office's proposed reforms, which exacerbate these flaws inherent in the IPA.

The IPA's existing authorities are broad and already pose a significant risk to the global availability of important security technologies. Under current law, the Home Office can issue a "Technical Capability Notice," that seeks to obligate a provider to remove an "electronic protection" to allow access to data that is otherwise unavailable due to encryption. In addition, the Home Office claims further authority to prohibit the provider from disclosing any information about such a requirement to its users or the public without the Secretary of State's express permission. Moreover, the IPA purports to apply extraterritorially, permitting the Home Office to assert that it may impose secret requirements on providers located in other countries and that apply to their users globally. Together, these provisions could be used to force a company like Apple, that would never build a backdoor, to publicly withdraw critical security features from the UK market, depriving UK users of these protections.

The reforms recently proposed by the Home Office seek to further expand the Secretary of State's authority and erode some of the protections originally included in the IPA. The new powers the Home Office seeks—expanded authority to regulate foreign companies and the ability to pre-screen and block innovative security technologies—could dramatically disrupt the global market for security technologies, putting users in the UK and around the world at greater risk.

We believe the following reforms proposed by the Home Office are highly problematic:

- *Pre-clearance requirement (Objective 4):* The Home Office proposes new authority that would allow the Secretary of State to require technology providers to pre-brief the Home Office of any changes to their offerings that could impact the UK government's ability to access user data. That would suppress innovation, stifle commerce, and—when combined with purported extraterritorial application—make the Home Office the de facto global arbiter of what level of data security and encryption are permissible.

- *Extraterritoriality (Objective 3):* The Home Office proposes that the extraterritorial scope of the IPA should apply to providers in any country, regardless of whether the provider has any physical presence in the United Kingdom. Under this proposal, it's possible that a non-UK company could be forced to undermine the security of all its users, simply because it has a UK user base, however small.

- *Requirement to maintain the status quo during the review process (Objective 1):* Currently, the Secretary of State must navigate important oversight mechanisms before she can block the offering of a new product or service she believes will impact the UK government's ability to access private user data. The Home Office now seeks to insert an end-run around these protections and proposes new authority to block, in secret, the release of a product or service even before a notice can be reviewed by independent oversight bodies. This upends the balance of authority and independent oversight Parliament struck in the IPA.

Taken as a whole, these changes amount to an expansion of the Investigatory Powers Act that would impinge the prerogative of other governments and rights of their citizens to determine for themselves the balance of data security and government access within their own jurisdictions.

The dangers in such an approach are obvious. It would be improper for the Home Office to act as the world's regulator of security technology, and its doing so could create serious conflicts of foreign law—including the

European Union's General Data Protection Regulation and the United States' CLOUD Act. In addition, a requirement to pre-clear emerging security technologies with the Home Office would dissuade any technology company that falls within the broad scope of the UK's assertion of authority from investing significant time, energy, and resources into developing new security technologies when the Home Office may summarily and secretly veto the use of those technologies. Finally, it is deeply troubling that the Home Office is seeking power to issue what are effectively secret extra-judicial injunctions against emerging security technologies without any recourse by the service provider.

Apple has long been committed to user privacy and security, developing and improving upon features to protect user data with innovations that give people greater insight into how their data is used and more powerful tools to protect it. Apple actively seeks to protect its users by designing security into the core of its platforms and using industry-leading security technologies to protect user data.

Apple has continued to enhance its security features over time because the threats to user information are relentless, pervasive, and evolving. Customers expect Apple to protect their personal data from bad actors who seek to access, steal, and use that data without a user's permission. Our efforts to stay ahead of those threats have only become more important as millions of gigabytes of personal data are stored in the cloud. As illustrated by a recent summary of data breach research, "The Rising Threat to Consumer Data in the Cloud", the need to enhance users' security is especially urgent today, as the total number of data breaches has more than tripled between 2013 and 2021, exposing 1.1 billion personal records across the globe in 2021 alone.

One of the most important security features available to protect personal information both on the device and in the cloud is end-to-end encryption. That encryption technology ensures that only users—and not the companies who provide cloud services—can access a user's personal data and communications. This technology provides an essential layer of additional security because it ensures that a malicious actor cannot obtain access to a user's data even if the actor is able to breach a cloud service provider's data centers. Thus, it is critical to shielding everyday citizens

from unlawful surveillance, identity theft, fraud, and data breaches, and it serves as an invaluable protection for journalists, human rights activists, and diplomats who may be targeted by malicious actors. The critical value of encryption—and end-to-end encryption in particular—is a key reason for the technology community's broad consensus in support of these features.

As explained in further detail below, Apple strongly objects to the proposals to provide the Home Office with the power to pre-clear and block emerging security technologies and to expand the IPA's extraterritorial reach.

Pre-Clearance Requirement (Objective 4)

The Home Office should not have the authority to require technology companies to provide advance notification of technological security innovations. Such an amendment to the IPA would permit the Home Office to block the introduction of new security technologies in the name of ensuring the UK government's access to individuals' personal data for law-enforcement and national-security purposes. Such power, coupled with the proposed expansion of the IPA's extraterritorial reach, would obviously stifle the development of security technology, including end-to-end encryption.

In effect, the UK seeks authority that no other country has — to prohibit a company from releasing a security feature unless the UK receives advance notice. The result, inevitably, is that a company must choose whether to subject itself to the preferences of the Home Office or deprive users around the world of critical security features. While the benefits of pre-clearance to the Home Office are obvious, the danger to human rights activists, journalists, and at-risk populations across the globe are even clearer.

We are particularly concerned that the Home Office could claim the authority to use the pre-clearance requirement, in combination with the proposed expansion of the IPA's extraterritorial scope and the proposed requirement to maintain the status quo during the review process, to thwart the development of end-to-end encryption technology. For companies like Apple that value the security of their users' data, the pre-clearance and

extraterritoriality proposals would result in an impossible choice between complying with a Home Office mandate to secretly install vulnerabilities into new security technologies (which Apple would never do), or to forgo development of those technologies altogether and sit on the sidelines as threats to users' data security continue to grow.

Extraterritoriality (Objective 3)

The Home Office's proposal to expand the IPA's extraterritoriality should be rejected. The Home Office should not have a basis for claiming authority to act as the global regulator for a foreign multinational technology company merely because its services are sold on UK soil or one of that company's corporate affiliates provides telecommunications services in the UK.

As the IPA currently stands, the Home Office may issue a notice to a non-UK company that provides telecommunications services in both the United Kingdom and in other jurisdictions. The Investigatory Powers (Technical Capability) Regulations 2018 do not purport to limit the effect of a notice served on a non-UK company to UK persons, meaning that the Home Office could attempt to assert the extreme position that its notice powers extend to all of a non-UK technology company's users worldwide, as long as a small number of UK users use the service. If the IPA were amended to allow the Home Office to ignore the differences between a legal entity doing business in the United Kingdom and one providing services worldwide, it would effectively empower the Home Office to become the global regulator for every technology company around the world with a single affiliate (whether located in the United Kingdom or not) that provides telecommunications services in the United Kingdom.

There is no reason why the UK should have the authority to decide for citizens of the world whether they can avail themselves of the proven security benefits that flow from end-to-end encryption. The balance between those interests is the topic of active debate in many countries and one on which a wide variety of constituents—governments, industry, civil society groups, privacy advocates, and security experts—have strong equities and deeply held views. Different countries will reach different answers to the competing policy questions that end-to-end encryption poses—and those answers should emerge through the democratic process, not through the unilateral decisions of one country's law

enforcement agency made in secret. Moreover, any attempt by the Home Office to use its extraterritorial powers to compel technology companies to weaken encryption technology will only strengthen the hands of malicious actors who seek to steal personal data for nefarious purposes.

The use of the IPA's notice regime to undermine encryption technology around the world would also create serious conflicts with foreign law. For example, Article 32 of the European Union's General Data Protection Regulation (GDPR) imposes a positive obligation on companies to implement technical and organizational measures to protect the privacy of their users' personal data. Recital 83 of the GDPR highlights that encryption is one means by which a company can meet its Article 32 obligations. Secretly installing backdoors in end-to-end encrypted technologies in order to comply with UK law for persons not subject to any lawful process would violate that obligation.

In addition, a notice requiring a US company like Apple to maintain the ability to decrypt data for any of its users worldwide would violate the US CLOUD Act and the implementing US-UK Data Access Agreement. The CLOUD Act forbids the use of data access agreements to mandate the decryption of user data. *See* 18 U.S.C. § 2523(b)(3). The implementing US-UK Data Access Agreement also prohibits the UK from seeking the personal information of US person. *See* Arts. 1.4, 1.6, 1.12, 4.3; *see also* 18 U.S.C. § 2523(b)(4)(A). But if the Home Office could compel Apple and other US technology companies to maintain the ability to decrypt user data currently protected by end-to-end encryption, it would effectively amend the US-UK Data Access Agreement to include a decryption mandate in violation of the CLOUD Act.

Expanding the extraterritoriality of the IPA's notice regime is even more troubling in light of the IPA's requirement that the recipient of a notice not disclose the notice's existence. By requiring non-UK technology companies to maintain the ability to produce unencrypted data for all of their users worldwide—without notifying their users of that ability—the IPA would include a worldwide gag order. That is deeply problematic, especially considering that the legal systems of most nations treat free speech as a fundamental individual right.

Requirement to Maintain Status Quo During the Review Process (Objective 1)

Finally, Apple objects to the Home Office's proposal to impose a general requirement to maintain the status quo throughout a notice review process.

Currently, the IPA provides for a review process to ensure that telecommunications operators receive at least some minimal process before an IPA notice can become binding. Those protections are especially important in light of the serious obligations that an IPA notice can impose. The statutory requirement that the Secretary of State engage in a consultation period with the relevant operator before a notice is issued ensures that the operator understands the requirements and effects of the notice. The consultation also offers an opportunity for the operator to provide an explanation of the technology and any other relevant information to the Secretary of State, who is statutorily obligated to take that information into account when determining the technical feasibility of the requirements in the IPA notice. *See* Ch. 8 of Interception of Communications Code of Practice.

The review process mandated by the IPA is a necessary pre-requisite to ensure that the obligations imposed by a notice are fair and lawful under UK law. The Technical Advisory Board (TAB) and a Judicial Commissioner must take into account any evidence and representation from the targeted operator and the Secretary of State and must issue conclusions that the Secretary of State, in turn, is then required to consider. Those determinations by the TAB (as to the technical requirements and financial consequences of the notice) and Judicial Commissioner (as to the proportionality of the notice) aid the Secretary of State in deciding whether the notice meets the statutory requirements of the IPA. This procedure is a necessary undertaking before any operator can be compelled to comply with an IPA notice.

The Home Office's proposed obligation that operators maintain the status quo during the review period would effectively nullify the carefully drafted and thoughtfully negotiated procedural protections contained in the text of the IPA. Under the proposal, the Secretary of State could issue a notice attempting to mandate that an operator block adoption of a new technology, even if the TAB later determines that the "technical requirements and the financial consequences" of the notice make maintenance of the status quo infeasible, s. 257(6), and even if the Judicial Commissioner concludes that blocking adoption of the new technology is

not "proportionate," s. 257(7). The resulting regime would thus give initial notices the same force as final notices that have undergone the IPA's full review process. A notice issued only with the views of the Secretary of State should not be expected to strike the balance required in the IPA between privacy, cybersecurity and valid national security objectives.

This modified process would stifle attempts to innovate encryption technology and would prevent companies from responding quickly to growing data security threats. Empowering the Secretary of State to effectively issue an unreviewable, extra-judicial injunction to prohibit the release of a new technology would force companies to withhold end-to-end encryption features or other new technologies from users, even in light of evolving threats to their users' data security. Malicious actors would have a significant advantage in threatening user data.

* * *

The Home Office's proposals to expand the IPA's extraterritorial reach and to grant itself the power to pre-clear and block emerging security technologies constitute a serious and direct threat to data security and information privacy. To ensure that individuals have the tools to respond to the ever-increasing threats to information security, the Home Office's proposal should be rejected.