Consumer Education & Awareness WG Working Document

Key messages: are behaviours & recommendations that need to be communicated to Consumers, Manufacturers, Retailers, Service Providers, Governments, Civil Society, Educational Institutions etc.

- **Delivery mechanisms:**
    - Educational and Awareness Campaign (to be developed outside of this initiative).
    - A website/repository where all the below information and relevant links are available.
        - To be highlighted in final report, potentially linked to in the ‘live label’ being discussed in the labelling WG.

Scope:

- The focus is on **household and business IoT devices** (ie., automated vehicles and smart cities are not included).
- In the first phase of the initiative, the key messages are designed in general terms **for all consumers** (specific messages to youth, seniors, etc. could be developed at a later stage).

This **Shared Responsibility Framework** broadly organizes the ideas into the demand side and the supply side who can work collaboratively over the lifecycle of the device:

- **Demand side:** broadly understood as the expectations on the consumers who are active users of the IoT device
- **Supply side:** a broader category of stakeholders who are either directly or indirectly involved in the supply chain of the device.
- **Rationale:** a Shared Responsibility Framework is used to illustrate how the two can collaborate to bridge the gap between the ideal situation/behaviours that are outlined for consumers and the status quo by engaging the diversity of actors (expertise/stakeholders/forces/incentives/trusted authorities).

[For each category there is up to 6 messages/behaviours/tips/recommendations and they are meant to roughly correspond/link between the five in the demand side with the points in the supply side]

Roll-up of Key Messages/Recommendations:

See table below

Mechanism Stage	Demand Side: Consumers	Supply Side: Manufacturers/Retailers/Service Providers/Government/Civil Society/Educational Institutions
Before Purchasing	1) **Make sure you understand what you are consenting to and how the device is collecting, using, and sharing your data**.	1) **Improve accessibility and content of privacy policies** (ie., provide clear answers on how the device is collecting, using, and sharing data).
	2) **Consider the lifecycle of the device and the support available** to keep your device in use for as long as possible (ie., verify availability and duration of security upgrades and patches and whether any subscription fees will be required to access support and add-ons).	2) **Use availability/duration of patches, updates and support as a selling feature and publicize this**, and clearly indicate whether any subscription fees will be required to access support and add-ons.
	3) **Check if there are any extra functions** (ie., is the device collecting data that is not needed and could create additional risk, such as cameras and mics in smart TVs).	3) **Clearly indicate/disclose all functions of the device and how to minimize additional risk** (ie., how to turn off unnecessary video and audio recording in your IoT devices).
	4) **Check if your device can operate with your other devices, if it works without internet connection, who can repair it, and if you can resell it** (ie., is it interoperable with only closed networks/platforms; will devices like smart lock, camera, fridge still function even if the internet is down; are repairs only available from authorized service providers; are there any restrictions on resale).	4) **Clearly indicate/disclose any limitations on use, operability, sale or repair of the device** (ie., is it interoperable with only closed networks/platforms; will devices like smart lock, camera, fridge still function even if the internet is down; are repairs only available from authorized service providers; are there any restrictions on resale).
	5) **Check for labels and standards, know what they mean and how they how they get updated** (ie., low cost devices may not possess the requisite certification. Proper labelling and certification	5) **Use certification/adherence to laws, standards and non-binding best practices as a selling feature** and publicize this.

	indicates that devices have been tested and meet certain industrial standards, and therefore carry less risk.).	
At Use/Issue	1) **Follow best practices for network setup and configuration**. This will help mitigate risk when using IoT devices (ie., change your online passwords regularly, use stronger passwords and set up two-factor authentication on personal devices. See UK IoT Guidelines for Consumers and their one-pager).	1) **Clearly layout the shared responsibility regarding the devices' security and assist consumers to setup their IoT networks in a way consistent with best practices** (ie., make the default setting consistent with best practices, and convey expectations of consumers' awareness/responsibility in the instructions/ToS/warning leaflet of the device).
	2) **Ensure that your whole network is secure and that your device's security is being updated automatically and regularly**. The security of your home network is only as good as its weakest link so make sure all your devices are always secure.	2) **Consider providing mechanisms to warn consumers when issues arise and remind them to follow the recommended security best practices** (ie., assist consumers in monitoring their traffic to detect anomalies, and follow recommended upgrading and patching recommendations from the NTIA Multistakeholder Process).
	3) **Be considerate of the privacy of your guests when they are in the vicinity of your IoT devices** (ie., when guests are in the proximity of your smart home devices, consider notifying them or turning devices off).	3) **Remind consumers about the effects of their IoT devices on their guests** (ie, audio or video recording).
	4) **Know where to seek redress or address technical problems or when your device has been hacked.** Manufacturers might offer a technical help service to consumers when they are having problems but familiarise yourself with other sources (ie., for privacy breaches contact the Office of the Privacy Commissioner of Canada), for security issues visit Get Cyber Safe, for copyright issues visit Office of Consumer Affairs, for product safety	4) **Provide transparent and accessible instructions on seeking redress**, and clearly indicate where to access this service and whether any costs are incurred when using this service (ie., Canadian Centre for Cyber Security).

	visit Health Canada for functionality and contract issues please contact the responsible Provincial authority).	
End of Life/Use	1) **Make sure to remove data from your device, and revert back to the factory default settings before disposing or moving**. There are many guides available to assist users with specific IoT devices (ie., Nest Thermostat http://www.imove.com/blog/how-to-switch-nest-thermostat-accounts-when-you-move/).	1) **Clearly indicate the best method or provide consumer assistance to permanently remove data from device and revert the device to factory default settings**.
	2) **Make sure to deactivate any older accounts that are linked with their devices.** (e.g. sometimes previous owners continuing to have control over thermostats and receive updates about them after they have moved out)	2) **Clearly indicate the best method or provide consumer assistance to get rid of previous accounts that are linked to their devices**.
	3) **Check the resources that are available to help responsibly dispose of IoT devices.** Retailors may provide this information.	3) **Provide sources to help consumers responsibly dispose of their IoT devices.**