Framework

A Framework for Digital Lifecycles and Consumer Protection

National Consumer Federation

@NCFvoice
nationalconsumer.org.uk

National Consumer Federation

With a focus on the digital privacy of consumer products

1. Introduction

If consumer protection is going to be provided through the often mentioned "Privacy by Design", consumers need to understand what is involved in order to do the job properly. It is much more than the initial design of a product, key though that is, and the aim is to provide a consumer view of what good lifecycle practice looks like for those designing and producing consumer products. And so this paper addresses a consumer understanding of product lifecycle processes in the digital world.

The framework embeds functional privacy protection into product design, then maintains and improves that protection over the product lifecycle.

This paper is a working document to be refined and improved through discussion with other consumer protection stakeholders.

A lifecycle framework that goes beyond privacy

Although this paper has been drafted specifically for privacy by design, the NCF is also working with Electrical Safety First to initiate work on digital safety by design. This paper is intended to be a contribution to that discussion and may be adapted as appropriate to the needs of product safety.

In addition to safety, the NCF will be working with other consumer stakeholders to examine the lifecycle framework's suitability for addressing further consumer needs 'by design', such as sustainability, accessibility and fairness.

2. Summary of design challenges for consumer products using digital technologies

2.1 Consumer protection considerations

The first priority of consumer protection for any product is its design and how it operates. In addition, consumer products need to be fair, safe, accessible, and sustainable. The way that products are understood and used by consumers varies considerably. The design of products needs to take into consideration the diversity of both users i.e. use by individuals with differing abilities, characteristics, vulnerabilities and accessibility needs and the different ways that such consumers actually use the products.

This paper provides a consumer view on what a responsible product organisation needs to put in place with respect to consumer product design and development to ensure consumer privacy protection is provided by its products. Privacy must be designed into the functionality of a consumer product and then maintained and improved over its lifecycle throughout the various types of lifecycle activity that directly involve the product.

2.2 The nature of consumer products that incorporate digital technology

Products incorporating digital technology
In addition to any consumer hardware provided, a consumer product's digital functionality may be implemented as

- code (software / firmware) residing in a piece of hardware that is a component of the product as a whole, or
- as separate software that runs on some existing consumer hardware already possessed by the consumer such as apps on smartphones, or
- as Software as a Service where the code runs on non-consumer i.e. organisational, computers somewhere across the Internet (Cloud services) such as online personal banking

Product organisations and liabilities
There is often misalignment and lack of clarity in responsibilities between component suppliers, main suppliers and end users[1] . A consumer view of key product organisation responsibilities is provided in sections 4.1 (across the lifecycle) and 5.1. (for specific lifecycle activities).

Rate of design change
With digital technology products, design change is frequent compared to hardware design changes. Minor updates may take place every few months, while major upgrades may be carried out every year or two. This means that assessment and testing of functionality, privacy controls, security and robustness of operation across many different use scenarios is difficult and is often expensive for each design level.

Many different digital technologies
Digital technology ranges from the relatively simple Radio Frequency Identification (RFID) 'tags' with low power and very limited processing capability to Artificial Intelligence (AI) where large computers are programmed to simulate neural networks with plenty of power and processing available to the AI implementation.

Diverse digital functionality sources
Not all software is custom designed for each product. Like hardware, software comes as components that can be sourced from others and incorporated into the software design of a product. When such components are 3rd party Cloud services providing software as a service, not only is design control more difficult, but these Cloud services may in turn use a cascade of software component functionality from other Cloud software services, elsewhere on the Internet.

Innovation in product design
Each year many thousands of new consumer products come on the market, with innovative digital design creating product types different from those of the pre-digital era.

---

[1] ENHANCING THE DIGITAL SECURITY OF PRODUCTS A POLICY DISCUSSION **OECD DIGITAL ECONOMY PAPERS** February 2021 No. 306 Section 2.1.3. https/www.oecd-ilibrary.org/docserver/cd9f9ebc-en.pdf?expires=1613143262&id=id&accname=guest&checksum=B65D6C1F58F7A001681410E2AFF1FC79

Digital connectivity and security
In addition to all the challenges above, the openness across the Internet has provided an opportunity for hugely more malicious use of products by 3rd parties exploiting human and technical vulnerabilities.

3. Strategic approach to Privacy by Design

In the UK, consumer protection in terms of product safety has been supported by product type safety specifications and testing standards. There are said to be about 4,500 of such British Standards. Taking the same product type route now would seem to be impractical, given the very fluid nature of consumer digital product design and the wide range of users, product types and digital technologies. Design change and innovation would always risk any product type standard quickly becoming out of date.

Our aim is to establish a generic consumer product digital design lifecycle framework that ensures the **right people** do the **right things** at the **right time** with the **right capabilities** in order to develop a product's design to build in protection for privacy for all that product's life, maintaining and improving design protection across a product's lifecycle whatever the lifecycle activities involved.

4. Overview of the lifecycle framework

Figure 1 below contains illustrative detail that is used throughout the rest of this paper. The figure illustrates the breadth and depth of lifecycle activity, and the considerations necessary for good lifecycle design practice.

The framework covers a number of elements:

- good practice that needs to be in place to enable the product organisation to address the whole lifecycle of a product
- good practices that need to be applied throughout the lifecycle for all product activities.
- good practices for particular lifecycle activities
- activities that should be the sole responsibility of the product responsible organisation Ref. sections 4.1 (across the lifecycle) and 5.1. (for specific lifecycle activities).

4.1 Good practice across the lifecycle

Good practice product organisations should provide clearly and directly :-

- accountability for product privacy performance (ref Figure 1 [1])
- product decisions from multi-disciplined, empowered and capable people who can deliver privacy by design (ref Figure 1 [1])

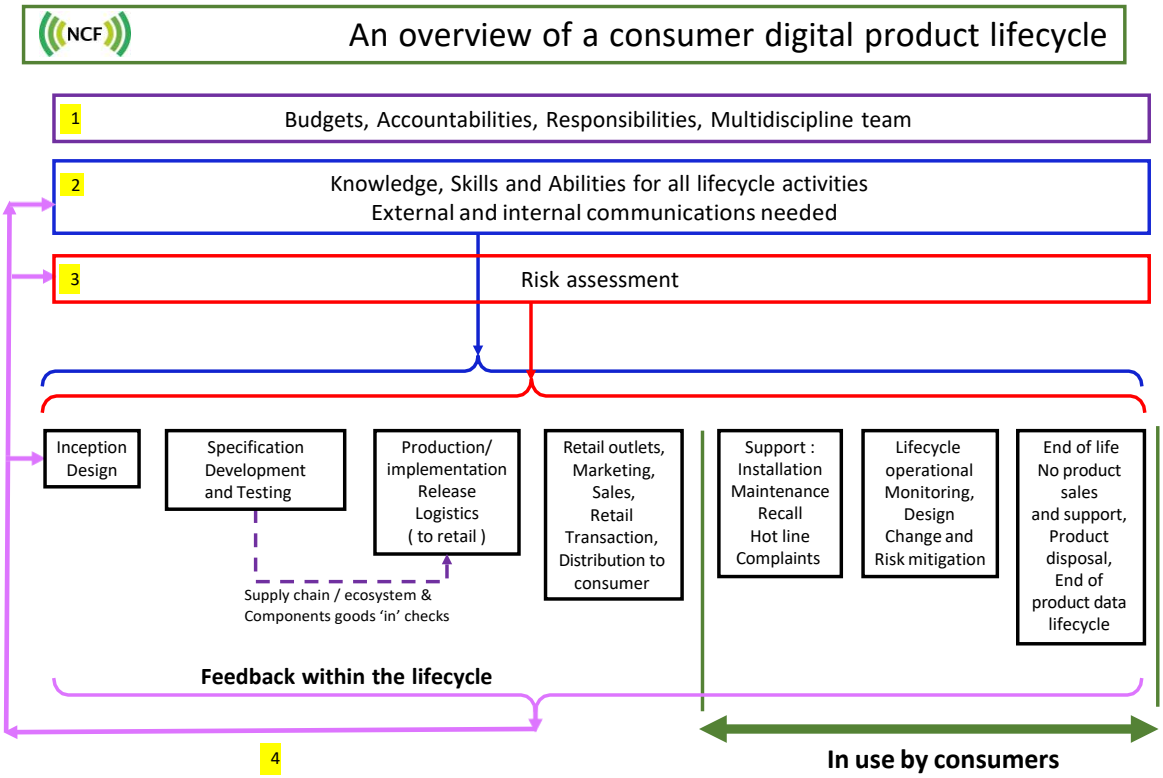
- having or acquiring the privacy-related knowledge needed by the product organisation to identify and undertake the right actions across the lifecycle, including internal and external communications (ref Figure 1 [2])
- privacy risk assessment throughout the lifecycle (ref Figure 1 [3])
- providing feedback mechanisms for all lifecycle activities to a product's multi-discipline team (ref Figure 1 [4])

4.1.1. Accountabilities, responsibilities, resources and multi-discipline working

If products are to be successful in meeting their privacy objectives, they need the right people involved in product decisions with the right levels of budget, resources and responsibilities/authorities to deliver those objectives.

Higher levels of management need to be accountable where they establish the objectives, as well as the accompanying resources. They must also assign responsibilities and authorities for multi-discipline team working with respect to the product's lifecycle operational activities.

Figure 1 – an overview of a consumer 'digital' product lifecycle



4.1.2. Knowledge and understanding of the lifecycle

In order to embed and maintain product privacy protection in a product's functionality and to maintain privacy associated with that product across its lifecycle, it is necessary that suitable action is taken with respect to the actual design of the product and the privacy protection associated with each lifecycle activity.

For this to be effective the following product lifecycle knowledge is needed:-

- a good product knowledge base for product privacy issues based on real life use, diverse types of consumer, their behaviours, capabilities, and privacy needs
- knowledge of previous or similar products
- information about design and technology issues (vulnerabilities and exploits) and good practice in avoiding or mitigating those issues,
- relevant regulations and standards and codes of practice
- detailed knowledge and insights into lifecycle activities and where privacy issues and concerns arise
- good means of keeping the lifecycle knowledge up to date.

4.1.3. Communications and feedback

The whole life approach to privacy by design depends greatly on the flow of good timely information between many parties.

During a product's lifecycle, consideration needs to be given to the privacy information that should be flowing out to, or back from, for example, consumers, post production ecosystems, component suppliers, as well as internal communications.

Outbound communications should ensure that consumers receive the right information at the right time and that each lifecycle activity receives the right information and any associated training and tools at an appropriate time.

Return communications are especially important for issues and problems relating to design and lifecycle activities and privacy protection which could need design change and/or mitigation action.

4.1.4. Lifecycle risk Assessment

One of the essential means by which privacy protection is designed into products and subsequently maintained and improved is through continuous risk assessment of design and the lifecycle activities.

Overall, product lifecycle knowledge and design inputs and feedback from lifecycle activities feed into privacy risk assessment. Risk assessment outputs then inform decisions taken through multi-discipline team working with respect to design changes and mitigation actions.

Good risk assessment needs to:

- build on cases for both the design and product use across the lifecycle for each lifecycle activity
- build on cases for known and reasonably foreseeable consumer use including consumers with diverse capabilities and behaviours, and known malicious activities.
- build on cases that are kept up to date with the latest product knowledge and lifecycle feedback.

Once risk has been assessed, decisions can be taken on design changes and / or mitigation actions. These actions may well need to be applied to different activities within a product's lifecycle.

5. Direct and indirect product organisation responsibility for individual lifecycle activities

5.1 Product Organisations

The specific lifecycle activities that product organisations should be directly responsible for are

- Design and development
- Sourcing components from 3rd parties and production of the product
- Consumer transaction terms and conditions that relate to the product's design and consumer protection (privacy, safety etc)
- Lifecycle operational monitoring (receiving feedback from internal and external sources)
- Design changes
- Risk mitigation action decisions
- End of product lifecycle actions (including the product's data lifecycle).

Product activities that occur post production may be undertaken directly by the product organisation, or by agents in a post-production ecosystem where control of such activities is less direct.

5.2 Product Ecosystems

When dealing with an ecosystem, the product organisation should be responsible for providing the wherewithal that should enable those 3rd parties in the ecosystem to be able to operate effectively in protecting consumers' privacy while undertaking direct product activities. For example

- Marketing
- Sales / Retail
- Distribution to the consumer
- Consumer support
- Installation
- Maintenance
- Complaints
- Retrofit
- End of life with respect to ecosystems or consumer use actions for product hardware and software

Where a product organisation undertakes any of the ecosystem lifecycle activities in 5.2 they bear the same responsibilities.

6. Lifecycle activities

6.1 . Initial product design

This should be the most influential activity for a product's overall design and one that determines much of how well a product can perform over its lifetime. The knowledge base for the product and its lifecycle is key. Ref section 4.1.2.

For really innovative products, initial design may be based on low product knowledge. In such cases knowledge should be built up actively with extended trials and testing and iteration with feedback to hone and refine the product's design while building the knowledge base.

The design work should provide key product privacy documentation for risk assessment and later lifecycle preparatory activities.

Initial design should yield product documentation such as :-

- A product description / definition making clear the design structure and all functionality being provided by the product
- Use cases for intended use and users, and other foreseeable and malicious misuse
- Product architecture and componentisation to identify 3rd party supply and own development
- Product operational data flows
- Identification of organisational infrastructure with which the product may need to operate such as point of sale payment terminals, QR codes etc.
- Identification of risks arising from 3rd party component functionality and any unused component functionality
- Identification of 3rd party products that interwork and are necessary for overall product functioning such as smart phones, home Wi-Fi routers, Internet services, personal computers and their browsers
- The privacy-maintaining interoperability needed with 3rd party products and any associated risks
- Personal and household product use with its privacy control requirements – functional and organisational
- Organisational lifecycle use, such as account creation, with relevant privacy controls
- Product security requirements.

6.2. Product specification, development and testing

Product specification should include requirements that create a design meeting consumers' privacy needs and expectations, relevant laws and regulations and any requirements of the product organisation.

Development builds on initial design and/or preliminary realisations to develop robust software code and/or hardware implementation.

During development, test specifications should be developed to ensure a product's design meets the intended capability, with validation against the requirements undertaken, before moving to design release for production.

Any design changes should be undertaken with full design change control so that the product organisation always knows what product design level it is dealing with. This is important from the consumer perspective since in later lifecycle activities, design upgrades and mitigations may need to be put in place where consumers are using a number of different release design levels.

In addition, development activities may include requirements for making use of specific design rules and the use of support facilities (like design aids, testers and simulators) when developing and validating the product's design.

Development should yield product privacy documentation such as

- A clear identification of the product's privacy capabilities
- e.g. product functional privacy preference controls and security controls
- The data types processed and, of those, the types of data that may provide personal identifiability.
- Data characterisation should include:
    - data input by users
    - the purposes for which that data is processed, identifying functionality and personal / household purposes, for example, geolocation functionality used for the purpose of finding a nearby restaurant, and also any organisational processing purposes
    - data created by the product within the domestic environment
    - data created by the product provider applications (processed on that provider's infrastructure)
    - data passed to or shared with 3rd parties
    - other data from 3rd parties processed by the product
    - where physically the product data processing is undertaken
    - where anonymised data contains linkable data types
- Test results and design validation to justify design release to production
- Risk assessment of the validated design level.

6.3 Production

Prior to production, the design level to be built needs to be authorised by those with product design authority to maintain design level control. The product organisation's production activities should also have a good understanding of their supply chain / supply ecosystem and have confidence in the hardware and software components supplied at 'goods in' in order to maintain inherent product design protection.

Components should be checked against those specified for the product to ensure product integrity as far as 3rd party supply is concerned. This is significant as changes to the components used in production can change privacy risks.

The final product build should also be checked to ensure the integrity of the production process itself. For instance, it has been known for software build to be infiltrated with malware within the code distributed to customers.

6.4 Release to market

For a product design to be released to market, all the necessary subsequent lifecycle activities should be primed and ready for dealing with the product, its customers and its users.

Also, at this point the product organisation should be fully informed of any regulatory or voluntary product assessments that should have been completed for the markets they are addressing and have those assessments completed and results available.

6.5. Logistics

Product hardware and software will be distributed to retail outlets through a number of different routes and mechanisms. This could be, for example, hardware shipping and input of the software build to software distribution servers.

Logistics activities may cause product information to be added to products and/or their packaging which could bring about privacy risks. Should such information still remain on packaging or in/on the product when it reaches the consumer, any associated privacy risks need to be assessed and where necessary mitigated.

Product distribution is another situation where infiltration of the product's design may occur, so in order to maintain inherent product protection, the organisation's logistics activities should demonstrate a good understanding of the organisation's distribution ecosystem and their confidence in the integrity of distribution and a means of monitoring for any privacy issues that may arise.

6.6. Marketing

Product marketing activity may be such that the privacy performance of a product influences consumer choice. To that end, privacy claims should be accurate and verifiable, with any significant high risks flagged to consumers in promotional material.

The organisation responsible for the product should provide relevant product privacy information to be used in marketing the product.

6.7. Sales

There may be a wide range of sales activities, ranging from a consumer with a sales person for complex products, through to online sales with no human support to the consumer, when the consumer is making their purchasing decision.

More privacy information may be required by the consumer before a commitment is made and the product responsible organisation should provide relevant product privacy information to be used with the consumer at point of sale. That information should be in an appropriate form for the nature of the sales activity. Consideration should also be given to providing sales support tools such as privacy demonstrations, videos etc.

Where sales people are to be part of sales activity, consideration should be given to their privacy knowledge and abilities and, where needed, the product responsible organisation should ensure that suitable privacy training is made available to them.

Where consumer 'off the shelf ' equipment is involved, privacy risk evaluation needs to take into consideration that retail outlets may have stock shelf life issues. This occurs where the design level in stock has fallen behind the latest design level available from the product organisation, in which case product action needs to be taken into consideration such as point of sale instructions to connect the product and download the latest software version prior to consumer use.

6.8. Consumer Transactions

For consumers who have privacy concerns, the transaction is a key lifecycle activity. Here agreement may be given for data collection and use beyond that necessary for the product's functionality - for example provided through the contract terms or via explicit consents.

Organisations' business models frequently involve the collection and use of consumer product data for purposes beyond the use needed within one of the product lifecycle activities. The product organisation needs to establish hardware terms and/or software licences during the transaction activity that are aligned, and are explicit, clear and transparent with respect to non-product lifecycle use of data.

This applies to both public and private sector consumer goods and services.

6.9 Distribution to the consumer

Consumer hardware and software can reach the consumer by different means. Examples are direct takeaway (from a retail outlet), a delivery service by hand or drone, or software download via the Internet.

Different means may involve different privacy risks e.g. would drone delivery use cameras and keep recordings of your home? Is there privacy-sensitive information on delivery packaging that encourages theft or discrimination? Have software distribution servers been infiltrated with malware, and so on.

So, a product organisation should have a good understanding of the distribution ecosystem to consumers and have confidence in the integrity of distribution. Where privacy risks in such activities have been identified, guidance and or operational instructions should be issued to members of the distribution ecosystem.

A means of gaining feedback from distribution to consumers' activities should be put in place to report back any privacy issues that may arise.

6.10. Market monitoring

4.10.1. Consumer use

While the early parts of a consumer product lifecycle should include a reasonable overview of consumer use, it is important to maintain a current view of how consumers are using the product and for what purposes.

It is not unknown for unexpected use to emerge and also for unanticipated vulnerabilities and exploits to become visible.

Privacy risks need to be reviewed continuously and updated in the light of ongoing monitoring of consumer use and product use.

An important feature of monitoring consumer use should be to provide the product responsible organisation with a view of the different product design levels in use by consumers. This is an influential factor for future design change, upgrades and design support decisions.

6.10.2. Other market monitoring features

In order to maintain consumer privacy protection in the context of a hostile digital environment, products should not be released into the market unless the product responsible organisation has in place the means to monitor the privacy performance of the product when in use. This requires communication channels for privacy issues and concerns to be in place for the public and professional worlds.

Such feedback communication channels should include consumer social media and complaints as well as feedback from all product support services (see section 6.11.) and independent professionals such as security experts, consumer bodies and regulators.

Actions resulting from market monitoring are dealt with in section 6.12. on design change and risk mitigation

6.11. Consumer product support

Product support plays an important role in a product's lifecycle, enabling consumers to keep using their products. Product support comes in many forms, such as

- installation (including self-installation)
- maintenance
- hot lines and Frequently Asked Questions (FAQs)
- software inbuilt 'help' and software upgrades.

The support provided for consumers who have problems is just as important, where the means for dealing with complaints, product returns, and ceasing service should be provided.

As addressed in section 4.1.3.,the product responsible organisation needs to ensure that all consumer product support activities are capable, in terms of qualifications and experience, documentation, training and equipment, of maintaining consumer privacy in their operations.

6.12. Design change and risk mitigation

Market monitoring information needs to be evaluated and genuine issues with any particular design level validated. Then decisions need to be taken on priorities and how to address the validated issues. Actions could include

- when urgent action is needed, for example with a major data breach at a processing centre, immediate information should be provided to those concerned with proactive measures & advice for consumers
- Urgent product corrective action leading to, for example, software fixes and or product recalls / retrofits and in worst cases withdrawal of the product from the market.
- where organisational product processing services have been compromised, internal organisational action to rectify security weaknesses and - where needed, - restoration of processing and data.
- scheduling requirements for design changes into future updates
- agreed action with 3rd party product or component providers where more rapid fixes may be possible until significant product design change can be developed, validated and released.

6.13. Design change and risk mitigation communications

When dealing with serious product privacy issues, consumer communication is key but may be constrained on occasions if public communication would alert malicious players to unfixed vulnerabilities of which they were not aware.

Subject to prioritisation by the scale of harm being caused, organisations should know which authorities to notify and should do so.

When mitigation action has been determined, all parties, including consumers and support services, should be informed and capable of taking the mitigation action needed. Action may be required in any of the lifecycle activities and all should be reviewed when determining design change and mitigation action communications.

Design changes should be developed, tested and validated before being released into the market and, where retrofit action is needed to change product design, to protect design integrity the product organisation should ensure that the support services involved have sources of valid hardware and software components.

6.14. End of lifecycle

There are many ‘end points”
in a product’s lifecycle that need to be taken into consideration for the privacy issues. The product organisation should take into account for example

- end of sales
- end of design upgrading i.e. no future design changes or software updates
- end of any or all support services
- end of the consumer use of a product – disposal, gifts / passing to another consumer, second hand markets, recycling.
- end of product data processing – it needs to be borne in mind that such data may be retained for a number of legitimate reasons for years after the end of a product’s sale.

All these ‘end points’ have different privacy implications which need to be evaluated and risk assessed with suitable consumer privacy protective actions taken by the product responsible organisation.

The product responsible organisation should ensure that end of life / use privacy protecting communications are provided to consumers and to all impacted lifecycle activities.

Peter Eisenegger Feb 2021
NCF Director Consumer Digital Concerns