Institut Mines-Télécom

Chair Values and Policies of Personal Information

Signs of trust

The impact of seals on personal data management

Coordinated by
Claire Levallois-Barth

January 2018

TELECOM ParisTech

TELECOM Ecole de Management

TELECOM SudParis

Signs of trust

The impact of seals on personal data management

How to cite this handbook: Signs of trust – The impact of seals on personal data management, Paris, Handbook 2 Chair Values and Policies of Personal Information, Coordinated by Claire Levallois-Barth, January, 2018.

http://www.personal-information.org/

ISBN 978-2-9557308-5-0 9782955730850 - electronic version - January, 2018

Table of contents

Introduction

Armen Khatchatourov

Trust, as the foundation of any society, sustains relationships among citizens as well as relations between individuals and organisations. It determines the very existence of institutional and commercial exchanges and questions the role these exchanges play in building a cohesive social body. We are currently experiencing a crisis of trust — or so is claimed — in the economic, political and social fields; a crisis most likely enabled by digital technologies, as these have disrupted both economic models and mechanisms underlying the public sphere.

More particularly, recent advances in the study of personal data flows pinpoint user mistrust towards both economic actors and state authorities. This issue is made even more complex by the specificity of digital goods (known as "credence goods" in economic theory), since consumers are not always aware of the "quality" of such goods, even after consumption.

In view of these developments, new regulation modes are emerging, from the multiple laws on "trust marks" or "seals" (through the General Data Protection Regulation, GDPR)[1] managed by public and/or private authorities, to crowd-sourced processes actually initiated by users (see TOSDR),[2] and *de facto* technical regulation (e.g. through ad blockers). One might consider such new modes as means to bridge the crisis of trust, yet for that purpose, the situation needs to be studied more carefully, through a multidisciplinary approach. An essential and problematic question, shared in their own way by several disciplines, is that of ***formalisation of trust***.

The concept of risk and its formal assessment are thus central to the economy, since trust is often associated with the risk consumers assign to their counterpart in a transaction. In this respect, in its poll records on digital trust, the French Digital Economy Association (ACSEL-CDC)[3] defines trust as the absence of such risk. Similarly, the reputation premium is calculated based on the difference between the price offered by a seller that pays all of their obligations to a buyer and the average price offered on the market for a similar ser-

1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), EUOJ, L 119, 4.5.2013, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

2 "Terms of Service; Didn't Read" https://tosdr.org/

3 Poll records on digital trust published by ACSEL-CDC, 2016 http://www.caissedesdepots.fr/sites/default/files/medias/barometre_de_la_confiance_des_francais_dans_le_numerique_0.pdf

vice. Reputation premiums can be awarded by experts that assess risks, such as Moody's or S&P with loan default risks, or by consumers that rate sellers on a marketplace, such as Amazon or eBay's.

Formalisation of trust in computer science also relies on risk assessment methods and the provision of unforgeable certified proof. Trust is classically qualified as "hard" or "soft", depending on the signs of trust provided: either strong cryptographic technical elements, or a collective assessment by several entities, with automated surveillance tools, of an entity's "normal" or "deviant" behaviour, just like reputation systems. "Hard" signs are always made up of cryptographic elements and proceed either from a trusted authority (or chain of authorities), as is the case with electronic certification and anonymous certification, or from a group of entities, as with the blockchain technology.

In law, trust is usually defined as the belief in one's good faith. The body of law is mainly used to protect vulnerable parties when the social ties preceding commercial exchanges are not old or strong enough for transactions to be carried out properly. However, it seems that digital transformation is now reorienting the legal approaches to building a new legal framework that ensures the effective operation of markets: rather than protecting vulnerable parties "*as individuals*", the aim is now to "*protect the economic function embodied [by these parties].*"[4] Thenceforward, is lawmaking on "trust" guided by the same processes (formalisation and risk assessment) than those observed in economics and computer science?

Finally, from a socio-philosophical perspective, one may infer that such formalisation of trust comes with its own specific risks. The example of personal data regulation seems to reveal a less significant role of the State, since the focus of regulation authority is moving from the legislative system to a new model that brings together the State, the market and the consumers in varying proportions. This evolution may either be interpreted as the State giving up on its ability to regulate certain aspects of digital technologies, or as its entering a constructive dialogue with non-State entities, some strictly private and others involving end-users. Either way, it seems to us that in the space opened in such a way, deliberation and dysfunction-correcting mechanisms are no longer adjusted to the political debate, but

4 Rochfeld, Judith. (2009). *De la «confiance» du consommateur ou du basculement d'un droit de protection de la partie faible à un droit de régulation du marché. Conférences du CEJEC, Approche critique du vocabulaire du droit européen : la confiance, Oct 2008,* France. pp. 7-11. <hal-00424954>

rather to the market model. Are the end-users still the citizens, or have they been replaced by consumers who “vote with the dollar”?

As regards daily uses, such evolution also impacts the actual constitution of individuals and citizens as well as their ability to act. The example of data protection seals is perfectly relevant in this respect, as it shows that digital transformation and the related datafication process deepen social tensions. Indeed, on the one hand, the expansion of seals may be seen as a step towards protection and empowerment, since users are better informed and their personal data is less exposed to capture. Yet, on the other hand, formalising trust, reducing it to external signs, suggesting preselected products and services, and ignoring fundamental trust-building mechanisms may well prevent us from achieving user empowerment. Again, emerging regulation modes are raising many new questions that need to be studied carefully.

In this handbook, we first introduce the transformations that trust and forms of trust are experiencing (Chapter 1 to 4). We then study the effects of such changes on the implementation of seals as external signs of trust, focusing on the role of public authorities (Chapter 5 to 8). We study the potential impacts of certification on economic actors and end-users (Chapters 9 and 10). Finally, through the example of blockchain, we inquire to what extent emerging technologies contribute to building trust (Chapter 11). Generally speaking, the question guiding our reflection is whether the theme of trust might raise societal issues that extend beyond risk management, total transparency, the fear of sanctions or the search of benefits.

How to cite this chapter: Khatchatourov A. “Introduction”, *in Signs of trust – The impact of seals on personal data management*, Paris, Handbook 2 Chair Values and Policies of Personal Information, Coordinated by Claire Levallois-Barth, January, 2018, pages 1–4.
http://www.personal-information.org/

Chapter 1.

Trust in digital environments: from external signs to the regulation of the self

Armen Khatchatourov

1

Our societies are becoming increasingly complex, as any public or private action requires taking into account various indices and factors, making any decision-making process more and more challenging. In such conditions, mechanisms that reduce complexity and support decision-making processes are becoming crucial. Niklas Luhmann, founder of the social systems theory and prominent sociologist of the second half of the 20th century, refers to “trust” as a major means of reducing uncertainty. Indeed, when you trust a particular actor, product, or service, you naturally start interacting with them more frequently, since your uncertainty about the outcome of the interaction is reduced.

Before going any further, we should more precisely depict the different issues at stake when it comes to trust. How does trust operate in a particular decision? Does it necessarily consist in calculating the consequences of an action, thus aiming to reduce the risk incurred? What coordinates the individual actor’s will with the institutional factors likely to influence it?

Trust in digital environments: from external signs to the regulation of the self

1.1. Confidence or trust?

One way to approach trust was conceived by Luhmann and consists in making a distinction between two different uncertainty-reducing mechanisms: *confidence*, which is based on assurance, and *trust*, which is based on decision.[1] Let us exemplify this distinction.

Suppose you are buying a second-hand car from a seller you do not know well; you are fairly uncertain about the product quality. You have to weigh up the pros and cons and make a rational decision based on plenty of factors: price attractiveness; your knowledge of mechanics; what you know about the seller; etc. You make a decision based on incomplete information and take a leap of faith, a moderate risk. You find yourself in a trust situation: in the end, you ***decide*** to trust the seller. In such situation, more information on the seller may make the decision-making process easier.

Now, let us say you drive that same car to work every day. As you get to a crossroads with heavy traffic, you also need to reduce your uncertainty that everything will go well. Yet, you do not constantly compare plenty of factors; rather, you rely on the fact that things going well is ***ensured***: life always goes its way, cars actually start up, and bridges usually

1 Luhmann, N. (2001). 'Familiarity, Confidence, Trust: Problems and Perspectives' in Gambetta, Diego (ed.) Trust: Making and Breaking Cooperative Relations, University of Oxford, Chapter 6, pp. 94-107.

don't fall down. Confidence is therefore "systemic": the whole system is working;[2] you don't need to start from scratch for every action you undertake.

The same logic can be applied to digital technologies. You decide to buy something on eBay to a highly- or low-rated seller and thus choose to *trust* them, yet your action also relies on *confidence* as regards how the whole thing goes, including the functioning of the eBay website, banking system, transportation, mail service, etc.

On another level, distinguishing between trust and confidence allows to address more complex — and perhaps more important — issues of our current society as a whole, which is undergoing a crisis of trust in politics, or rather in all social interactions, according to some. Indeed, one can trust such or such political actor by making rational calculations of the benefits one can obtain individually. Yet this trust in a political actor cannot predict the confidence one may have in the political system they are a part of, in the social cohesion of the whole.

Confidence and trust thus reduce the situational complexity individuals may face, allowing them to take action in situations of uncertainty and unfamiliarity. However, confidence and trust operate in fundamentally different ways. Such differences can be understood along two axes:

- (a) The first axis relates to the mechanisms involved in building trust and confidence, and the part given to actors' rational behaviour.
  - As regards trust, what matters is the decision made by an informed individual — or who has at least carried out a rational risk assessment;
  - As regards confidence, these mechanisms are institutionalised; and in an interaction, rational decisions matter less than socially acquired habits. The local grass-roots network of interactions is what helps things go "naturally" and establish confidence. In this sense, confidence is related to the long history of social interactions as it cannot be decided from the top down, cannot be forced, and its facilitating mechanisms are more complex to formalise

(a)

2 We believe this has led to confusion for some authors, as they limit confidence to confiding in technical systems or institutions, whereas for Luhmann confidence refers to a mindset, not a specific object. Some also seem to define it as blind confidence (possibly in systems), whereas confidence is based on a logic and time scale that differ from risk calculation.

- (b) The second is about how individual actors guide their future behaviour. This can be seen as some kind of feedback loop in which a given action determines future action.
  - In the case of confidence, the failure of one particular action is attributed to external factors over which actors have little control; what is at stake is the system as a whole. Coming back to the example of the second-hand car, one would say that to understand why an incident happened, you have to understand how the whole system, with the sellers, road constructors and traffic regulators, in their own history and context, is at stake.
  - In the case of trust, failure is attributed to the actual individual's behaviour and "wrong" calculations. Coming back to the example of the second-hand car, one would say, "I should not have bought this car; I'm the one who made wrong calculations". Trust is thus only possible if actors agree they might face non-transparency and possible losses. Full transparency — if it could happen at all — would then only be possible thanks to mechanisms other than trust.

Making such a distinction has a very simple reason: attributing one's failure to oneself is the very basis of the concept of ***risk*** and of the fact that calculating risks is an operation internal to an individual trying to work out external factors. Yet this distinction cannot be underestimated. Indeed, focusing on trust does not only mean focusing on a behaviour that matches the individual's rational decision at a given time; rather, trust also conditions the way individual behaviours will be guided in the future. In other words, what is at work here is the self-governance mechanism, which makes individuals become who they are. As we explain later, the mechanism of self-attributing failure, which ***responsibilises individuals***, is dominant today.

Before going more into detail about the digital evolution, let us concisely formulate the question underlying our reflection: admitting we are going through a "crisis of trust", especially towards companies or states that collect and use our personal data, are we actually facing a crisis of *trust* or a crisis of *confidence*? If public policies and private entities are aiming to strengthen "trust" in digital technologies, which of the two should they prioritise?

1.2. **A brief history of trust**

Let us first stress that historically, major technological evolutions have influenced the repartition between confidence and trust.

According to Luhmann, the invention of printing allowed to spread knowledge and reduce the distinction between the familiar and the unfamiliar. Religious *habitus*, which had guided daily action until then, was disrupted. Assessing individual action and taking part in the whole of society then became primordial stakes. Such rise of the individual in society is precisely what gave rise to the need to coordinate confidence and trust. Based on this historical breach, Luhmann makes this schematic distinction: in an increasingly complex world where individuals are required to make decisions, trust would be used to reduce complexity and make one-off decisions (on interpersonal relations, calculated risks) while confidence would be involved when individuals take part in the whole of the economic and political system. It should be specified that trust and confidence are not part of the same temporality, since trust is a matter of event while confidence is continuous.[3] The actual repartition between trust and confidence is therefore the result of a long historical process. "Trust" does not have an organisational or psychological reality outside of the frame of social changes.

Closer to our time, liberalism and neoliberalism both carry on that movement, as they emphasise trust. Indeed, insofar as society is seen as a group of autonomous, free and liable actors that calculate potential risks and benefits, societies emphasise their reliance on mechanisms of trust, perhaps at the expense of confidence and its understanding. However, as Luhmann points out, while a lack of trust may withdraw individual activities and risk-taking decisions (regarding investments, purchases, consent to personal data collection and use, etc.), a lack of confidence might lead to "*a diffuse sentiment of dissatisfaction and alienation or even anomie.*"[4]

---

3 Confidence and trust thus meet two different kinds of uncertainty, "uncertainty within the event temporality and uncertainty […] within the continuity temporality", cf. Morten, Frederiksen. (2016). Divided uncertainty: A phenomenology of trust, risk and confidence, in Søren Jagd and Lars Fuglsang (ed.) Trust, Organizations and Social Interaction. Elgar.

4 In sociology, anomie is traditionally characterised as the absence of norms and a disintegration of the social order.

« The lack of confidence will lead to feelings of alienation, and eventually to retreat into smaller worlds of purely local importance to new forms of 'ethnogenesis', to a fashionable longing for an independent if modest living, to fundamentalist attitudes or other forms of retotalising milieus and 'life-worlds'.»[5]

These feelings of alienation do not only negatively impact the trust one may have while carrying out occasional activities, but also on one's (feeling of) belonging to society.[6] In other words, emphasising trust means disregarding the fact that trust relies on confidence, which is one of its most essential conditions.

Taking Luhmann's stance even further, we may infer that trust itself does not have the same conditions of possibility *per se*; and always presupposes a basis rooted in social, grassroots interactions. Money is an example of such. One trusts (opposing confidence as much as one likes) money because others trust it and because money is the result of a long institutional history of exchanges. As Gambetta put it in the title of his famous article "Can we trust trust?" in 2000, one can indeed trust trust, yet such phrase has to be complemented: we can trust trust, provided that confidence processes are also involved.

It therefore appears that trust is simultaneously an economic, technological, regulatory, and fundamentally social issue when it comes to its consequences. Besides, it seems incorrect to refer to a "crisis of trust" as if it were a mere quantitative change — there is less trust today than there was yesterday — and as if it was only a matter of implementing carefully chosen action to restore the level we have lost. Rather, as we are trying to demonstrate, it is a change in the governance regime of stakeholders and in how individuals build themselves through their own choices.[7]

---

5 Luhmann, N. (2001). 'Familiarity, Confidence, Trust: Problems and Perspectives' in Gambetta, Diego (ed.) Trust: Making and Breaking Cooperative Relations, University of Oxford, chapter 6, pp. 94-107

6 On this matter, Louis Quéré refers to a "general disposition to belong." Quéré, L. (2001). *La structure cognitive et normative de la confiance,* p. 141.

7 See Khatchatourov A., et Chardel, P.-A. (2016). *La construction de l'identité dans la société contemporaine : enjeux théoriques. in « Identités numériques », Cahier n°1 de la Chaire Valeurs et Politiques des Informations Personnelles,* coordinated by Claire Levallois-Barth.

1.3. Can we trust digital environments?

The digital transformation is adding another layer of complexity to these issues. Based on what has been said so far, one can assume the issue here is not simply the reduction of "trust" in the current situation where digital interactions are increasingly replacing classical interactions. Rather, a new repartition between trust and confidence mechanisms is under way. As such, the issue of trust is closely related to that of identity and to modalities according to which the "autonomy" of an individual develops through the decisions they make.

Let us come back to the two axes we mentioned earlier, i.e. (a) the role of local interactions and (b) the mechanisms of failure attribution.

It seems that in the current situation, where the neoliberalist regulation of economic activities prevails and digital technologies are rising, while their respective parts cannot be clearly outlined, the movement described by Luhmann is being strengthened.

- (a) Risk calculation is supplanting local interactions in two ways. First of all, risk calculation and the decision-making process it implies are drifting away from local interactions. The calculation is often nudged by centralised regulation authorities that legitimise economic or institutional actors, thus promoting some actors to the detriment of others. For instance, in IT, as long as trust is addressed only from the angle of security, the emphasis is on very specific risks, such as identity theft, to the detriment of other social issues, such as the consequences of generalised surveillance. In doing so, some risks and the economic and institutional actors they are related to are prioritised, as shows the primacy of security over privacy. Second, risk calculation is being increasingly formalised as it is now relying not on public debate or deliberative legislation (be it based on trust or confidence), but on formal algorithms, which can actually reduce consensus and social cohesion.[8]

- (b) Activity results are more and more assigned to individuals/users, so the feedback loop keeps getting tighter, even in daily activities. For instance, let us say you are going for a run with your FitBit tracker and you analyse your data or make it

8 See Rouvroy, A. & Berns, T. (2013). Algorithmic governmentality and prospects of emancipation: Disparateness as a precondition for individuation through relationships? Réseaux, vol. no 177, no. 1, 2013, pp. 163-196

public, because your insurance or social security reimbursements depend on it; at the same time, you are also required to reduce global health expenses and make society economically thriving. In this case, precisely because individuals seem to be seeking well-being among a choice of options which they are required to trust (as in, to rationally decide to trust), they are made accountable for the consequences of their actions and they thus comply with the pre-established feedback loop. However, since their choice is itself defined by external bodies, individuals are "trained" to take responsibility without feeling concerned about the fact that they are not actually accountable for the menu of actions they are given. We may infer, based on Michel Foucault's works, that society is trying to make citizens "responsible" through sanctions and rewards.[9]

This is one of the drawbacks to the so-called informational self-determination approach[10] in contemporary society, where users have to trust preselected actors that are legitimised following processes they most often cannot understand.[11] Stating that individuals are accountable for their decisions leads to a kind of "*contractualisation of common life*",[12] where the effects of one-off decisions on the constitution of subjectivity are not questioned. For users, choosing a service over another means "self-managing" in one-off actions and taking responsibility for costs and associated "risks".

The paradox we are currently facing is that while individuals are being ***made responsible***, they are also being ***deresponsibilised***. Indeed, since they are required to fully comply with orders and signs coming from external authorities, individuals face the risk of lacking necessary critical skills, thus jeopardising the Enlightenment project of autonomous individuals. For instance, will generalising digital service certification not lead to generalising

9 See Philippe Fournier on the example of social policies: "Risk management, children's education, the neighbourhood you live in, and so on, are all factors related to individual responsibility. In the end, individuals who seem to deny responsibility, i.e. who do not take part in optimising the people's well-being [...], are punished, disciplined or merely left out." (Fournier, P. (2015). *La responsabilité comme mode de gouvernement néolibéral : l'exemple des programmes d'aide aux familles aux États-Unis de 1980 à nos jours. in Les ateliers de l'éthique, Volume 10, Numéro 1, Hiver 2015*, p. 129–154) [Unofficial translation from the original French]

10 This approach originated in Germany in the 1980s; it has been echoed in the General Data Protection Regulation.

11 This point, especially the practical example of certifying digital actors, is explained more in depth in the following chapters.

12 Foucault, M. (2004). 'The Birth of Biopolitics', in: Michel Foucault, Ethics: Subjectivity and Truth, ed. by Paul Rabinow, New York: The New Press 1997, pp. 73-79.

stereotyped behaviours, as individuals merely follow orders while clearing their conscience by supporting actors that also blindly comply with formal data protection prescriptions?

Let us summarise this new situation by stating the following: while the "exterior" of confidence used to be imputable to the *habitus* based on social interactions, it has now become an authority (legal or not) that nudges "rational" and "trustful" behaviours, now pertaining to trust. Yet as "rational" as these authorities might be, their creation and legitimising mechanisms are not much displayed.

Sociology since Max Weber has faced the following issue: how can legitimation processes — that decide which actors are trustworthy — be made accountable? How are behaviours (related to trust or to economic, political and social choices) prescribed? To such questions, we might add: how may trust become a specific regulation regime? Finally, and more specifically: how is trust — or even a "*suggested*" kind of trust — replacing confidence?

In this respect, Luhmann introduced the concept of legitimation by procedure.[13] Nowadays, procedures are increasingly relying on digital technologies, and the legitimation machinery, because data flows are being generalised, is becoming more and more obscure.[14] Let us define two possible — and problematic — configurations for this new kind of "suggested" trust: trust by design and distributed trust.

1.4. The mirage of trust by design: an illusion

Let us recall the two trends that emphasise trust over confidence, which we have explained in points (a) and (b) above. They are nowadays closely tied to a specific ideology: that of an "entirely technological" society in which technical, or to the very least techno-managerial, solutions are supposedly able to replace social construction. For instance,

---

13 To put it simply, *legitimation by procedure* is a concept according to which legitimacy is provided by the procedure of its own execution, since law is its own foundation (it has no divine or sovereign foundation). Procedure is therefore not a negative thing, rather the very mechanism through which law self-legitimises and acquires validity. Luhmann's *Legitimation by Procedure* focuses on three procedures: the settings of elections, parliament and court of law. These procedures are obviously being substantially changed by digital technologies nowadays, and their trust towards themselves or the actors involved is therefore also undergoing major changes.

14 For a more philosophical approach on the issues such flows may entail nowadays, see Khatchatourov A., (2016) *Big Data entre archive et diagramme. Études Digitales n°2*, Classiques Garnier, Paris.

algorithmic transparency is being praised as a sufficient solution for economic recovery, or even for social equilibrium, while the larger processes of algorithm design and effective use are left aside.[15] What is also not displayed is that regular users are not able to assess algorithms; they would need to trust other bodies — such as trusted third parties — that would be responsible for this, thus creating an infinite loop of actor legitimation, while the mechanisms of such legitimation are yet to be examined. Similarly, one might think implementing some kind of blockchain approach would help building trust between actors through a total transparency of exchanges, without analysing conflicts, oligopolistic stances, underlying political stakes, etc.[16]

Such ideology may be called “trust by design”.

Can trust be regained by making code and/or data more transparent, open and decentralised? Should we rather “trust” actors that we are familiar with and we believe are respecting our privacy, without having to put increasing efforts into protecting our data, or rather actors that provide technical solutions that seem to comply, here and now, with the formal requirements of this so-called “trust by design”?

Our point is that this movement of trust by design carries a fundamental ambiguity and emphasises trust even more over confidence. Individuals/users are required to make even more choices — which are preselected by external authorities —, even more data flows, and maybe even more data protection, yet they are losing the feeling or the guarantee they are taking part in a social whole.

Indeed, referring to the two examples we mentioned above, supposing the risk of data disclosure that comes with subscribing to a service is reduced, and supposing trust is “regained”, there is nothing we can say about confidence and its social construction.

There is more. The trend of using “trust by design” fundamentally raises the issue of automated trust and the automated production of its external signs with which individual

15 See Khatchatourov A. (2016). *Peut-on mettre la main sur les algorithmes ? Note sur la « culture algorithmique » de Dourish. Études Digitales, n°2*, Classiques Garnier, Paris.

16 More on this is developed in Chapter 11, which focuses on trust in blockchains.

behaviours are supposed to comply. Yet, as IT engineers very much know,[17] and as philosophy also keeps underlining,[18] the more essential question is that of the "deautomatisation", disengagement and suspension of common sense and common places; i.e. of critical thinking on these signs. This is the essential condition of democracy, or at least of the Enlightenment project. In this respect, as Luhmann also often stated,[19] a society can only function if a certain degree of distrust prevents trust from becoming blind trust, so that the *habitus* does not become an automatic reflex.

1.5. On "distributed" trust

Implementing public or business policies reducing what Luhmann calls alienation requires to preserve — or profoundly rethink — the fragile balance between trust and confidence. Otherwise, individual actions guided by trust might get blocked as well. Indeed, risk-taking is a structural necessity — both for the economy and for politics — yet it must be coordinated with confidence, whose mechanisms have nothing to do with calculation and prescription. By mixing trust and confidence and shifting the focus to trust, trust by design might well lead to an even greater disruption of confidence.

The issue therefore seems to be: how can we design policies — trust policies, trust-building policies, certification policies to "display" trust — that to the very least do not disrupt this balance nor reduce confidence building to risk-assessment mechanisms which merely "function" locally only to boost competition? In this respect, Chapter 2 addresses law and its twofold functional role, which consists not only in ensuring protection for weaker parties (historically, this function does not only regard economic mechanisms), but also in taking part in the market, regulating and boosting competition. A relevant example of this is the recent law on data portability, which aims to comply with the double bind of protecting (or empowering) consumers by giving them a certain control over their data, and to boost competition among providers by making it easier for consumers to switch from one to another and move their data. The issue is now to find out under which conditions institutional

17 E.g. with critical systems management automation (planes, nuclear plants, etc.), the main issue is not to automate "too much", so as to create a dynamic back-and-forth movement between automation and human control. Parasuraman, R., Mouloua, M., & Molloy, R. (1996). Effects of adaptive task allocation on monitoring of automated systems. in Human Factors: The Journal of the Human Factors and Ergonomics Society, 38(4), 665-679.

18 In Plato, the creation of Western philosophy is actually based on the suspension of judgment.

19 Luhmann, N. (1979). Trust and Power, Chichester: Wiley, 1979.

processes aimed at legitimising actors might not break away from the social processes related to confidence.

Let us point out that even economics, whose fundamental epistemological tenets are more compatible with trust than with confidence — i.e., with individual actors than with social processes — are beginning to point to this social layer of interactions which they had been overlooking. The following chapters thus address the fairly recent interest that has arisen in economics for notions such as “fairness” and “reciprocity” (see “Trust through fairness and reciprocity”, page 42), or repeated interactions.

We should therefore start reflecting on how to include citizens in these processes. Yet, the lesson we have learned here is that they must not be included in just any way. The rise of participatory, collaborative, distributed, mass-mobilising systems points to something of that kind. Plenty of mechanisms nowadays are initiated by individuals/users: crowdsourcing;[20] or the use of ad blockers by users, that operates de facto a technical regulation by imposing sanctions on Internet actors.

Yet the very terminological confusion in which such initiatives are trapped shows that the covered spectrum is too wide to comply with the requirements of confidence we mentioned. Indeed, what would be common to buyers that rank sellers on eBay and processes through which members of the free and open-source software community gain legitimacy among their pairs? Admittedly, both legitimation procedures are both contributing to reducing uncertainty towards a given actor. However, the procedures at work in the case of free software seem to be giving way to processes that partly look like confidence,[21] while the eBay procedure now seems to rely mainly on trust.

---

20 See for instance TOSDR: “Terms of Service; Didn’t Read”, https://tosdr.org/

21 As shown by O’Neil (2014) in Hacking Weber: Legitimacy, critique, and trust in peer production, “Legitimate domination in collaborative online projects was defined as overlapping regimes of hacker charismatic, index-charismatic and procedural authority which coexist in hybrid formations.” This form seems to rely on trust - choosing open source may be rationally justified by trust in the product quality and by personal recognition ambitions — as well as on confidence — at least as regards community members. In O’Neil’s quote, the term “index-charismatic authority” refers to an algorithm component, i.e. an automated “authority” calculation in a network, on which Barabàsi did pioneering work (see Barabàsi, AL. (2002). Linked: The New Science of Networks, Perseus, Cambridge, MA), while “procedural authority” seems to relate more to legitimation by procedure, even though Luhmann is not mentioned. Both kinds can therefore coexist and be distributed in varying proportions.

What now needs to be done is to think up ways to not only let ***consumers*** have their say — their functional role in the social system seems limited to trust — yet also set up processes involving ***citizens*** in confidence.

Such are the issues we believe are raised by the subject of trust in digital technologies: a new way of coordinating trust and confidence, responsibilisation and deresponsibilisation, reasoned trust and distrust. Addressing this issue is going to be extremely difficult. It is obviously not about abandoning any kind of regulation and letting individuals/users face the numerous data grabbers alone. Rather, it is about finding a critical approach to regulation, which would not over regulate citizen's behaviours nor become a part of "privacy washing".

How to cite this chapter: Khatchatourov A. "Trust in digital environments: from external signs to the regulation of the self", *in Signs of trust – The impact of seals on personal data management*, Paris, Handbook 2 Chair Values and Policies of Personal Information, Coordinated by Claire Levallois-Barth, January, 2018, chapter 1, pages 5–18.

http://www.personal-information.org/

Cover illustration: « La Confiance », pastel by Thierry Citron (www.thierrycitron.fr)

Chapter 2. Trust as embraced by law

Claire Levallois-Barth

2

Draft law on trust in politics, law on confidence in the Digital Economy (LCEN),[1] regulation (EU) on electronic identification and trust services for electronic transactions in the internal market[2]… as many legal texts that aim to strengthen trust. These seem to provide an answer to the crisis of trust that is affecting democratic institutions and their ability to solve citizens' complex problems as well as all risk-inducing technologies and businesses that seem more and more threatening.

However, and quite surprisingly so, the notion of trust has not been explicitly defined in French law. No bill has ever characterised this vague concept, (2.1) which actually carries a double role as regards data protection (2.2.). Outward signs of trust include seals, subject to both hard and soft regulation (2.3), and which differ from certification and marks (2.4.).

1 Law No. 2004-575 of 21 June 2004, regarding Confidence in the Digital Economy, OJ of the French Republic of 22 June 2004.

2 Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS Regulation), EUOJ L 257, 28.8.2014, p. 73–114.

Trust as embraced by law

2.1. The notion of trust

In the absence of a legal definition of the notion of trust, one may turn to doctrine. Gérard Cornu, Dean of the French Law Faculty of Poitiers, gives the following definition in his legal dictionary *Vocabulaire juridique*:[3]

Trust

1. The belief in one's (third party or contractor) good faith, fairness, sincerity and faithfulness or in their abilities, skills and professional qualifications (i.e. trusting a doctor);
2. The act of having faith in someone, more specifically entrusting them with a mission.

This is rather the common sense meaning than an actual legal definition, implying that trust is defined in reference to a person. Trust is an act of investing that person with a mis-

3 Cornu, G., (2016). *Vocabulaire juridique, Paris, PUF, 11e édition, 2016, V° Confiance*. [Unofficial translation from the French]

sion, such as a mandate[4] or a deposit[5] in special contract law. In French public health law, trust also refers to the possibility for any patient over age 18 to appoint a trusted person as their health care proxy, who will be consulted should the patient be unable to communicate their wishes directly and to receive the information necessary for this purpose.[6] If it is the wish of the patient, the trusted person may accompany them at every step and be present at medical appointments to help them make decisions.

Trust towards a person is also meant as a "belief" — as in, having faith in or giving credit to a relative, friend, expert or professional. In that sense, trust would be defined in relation to other notions, such as faithfulness in a marriage, the loyalty of an employee who should not go against the company's interests (e.g. by using available tools for personal use or selling trade secrets to competitors), or good faith while signing a contract. In the event one of the contractors has not — or has poorly — complied with obligations, one characterises their behaviour as "bad faith".

Trust can therefore also be defined in a negative way, through concepts such as the loss of trust and confidence in labour law or breach of trust in criminal law. A breach of trust is the wrongful misappropriation of any fund or property, in a way that was not consented to by the owner.

► In a decision dated 22 October 2014, the Criminal Chamber of the French Court of *Cassation* (the highest court in the French judiciary, civil, commercial, social or criminal cases) ruled as a breach of trust the fact that an employee had "*knowingly copied and misappropriated for his personal use, [at the expense of his employer], computer files containing confidential information provided to him by his employer for professional use.*"[7]

Aside from trust towards a person, law also plays a part in building confidence towards institutions. In EU law, ***legitimate expectation*** refers to the predictability and stability citi-

4 In French law, a mandate is a contract by which one person (the mandant) gives power to another (the mandatary) to do one or several legal acts for him and in his name.

5 In French law, a deposit is a convention by which a person, the bailee, receives and preserves the property or money of another person, the bailor, without reward.

6 Law No. 2002-303 of 4 March 2002 on patients' rights and the quality of the health system, OJ of the French Republic of 5 March 2002.

7 French Court of *Cassation*, Criminal Chamber, 22.10.2014, n°13-82.630.

zens may expect of standards issued by European and national authorities; while in budget law, the sincerity principle provides that "*the budget acts give a faithful representation of all the State's resources and charges.*"[8]

Finally, lawmakers seek to create an environment for trust towards companies, especially in the digital area, in which one cannot rely on old and established social practices.

It is worth noting that none of the French or European texts that include the terms of ***trust and confidence*** in their titles have defined these notions, be it the EU eIDAS Regulation on electronic identification and trust services for electronic transactions in the internal market[9] or the Law on ***Confidence*** in the Digital Economy (LCEN) of 21 June 2004. In the latter, the word "confidence", which was added at the very last moment to the actual title of the law, seems to refer to ***confidence as a psychological process***, as asserted by the Parliament.[10] Even though the titles state that they are a Law "on" Digital Confidence and a Regulation "on" trust services, both texts mainly aim to regulate the electronic commerce market. For that purpose, they both implement mechanisms aimed at warding off any risks users may perceive towards the global scope of new technologies, so as to ensure a "reassuring" experience making up for the lack of social links (see Chapter 1).

Here, trust is intertwined with the notions of security — whether legal, technical or organisational (e.g. through product and service certification, as we will see in Chapter 4) — and liability of actors of the digital economy,[11] especially technical service providers. "*Is being liable not being accountable for something? And is holding someone accountable for a given situation not a way of creating trust?*"[12] Legal regulation thus makes for a set of liability mechanisms and can therefore be seen as a trust-building tool.

---

8 Art. 32 of Organic Law No. 2001-692 of 1 August 2001 on budget acts, OJ of the French Republic of 2 August 2001.

9 See Castets-Renard, C., (2006). *Le formalisme du contrat électronique ou la confiance décrétée*, Defrénois, 30/10/2006, n°20, p. 1529.

10 See Castets-Renard, C., (2006). *Le formalisme du contrat électronique ou la confiance décrétée*, Defrénois, 30/10/2006, n°20, p. 1529.

11 Agosti, P., Caprioli, E.A., (2005). *La confiance dans l'économie numérique (Commentaires de certains aspects de la loi pour la confiance dans l'économie numérique) (LCEN), Petites affiches*, 03/06/2005, n°110, p. 3.

12 Vivant, M., (2004). *Entre ancien et nouveau, une quête désordonnée de confiance pour l'économie numérique, Cahier Lamy. Droit de l'informatique et des réseaux, n°171, juillet 2004*, p. 2 et s.

Consequently, in the field of digital technologies, trust is also closely tied to other notions, especially ones relating to data protection: the ***security*** of networks and information; the ***liability*** of data controllers and processors; as well as ***fairness***. Fairness is actually mentioned in many texts,[13] even though there is no legal definition of the ***principle of fairness*** either. Fairness is for judges and the CNIL to assess; it is meant — at the collection level mainly — as an obligation of transparency towards the people whose data is collected and processed. People thus have to be informed of who the data processor is, what the purpose of the processing is, what their rights are, etc. If they are not, Article 226-18 of the French Penal Code provides that "*the collection of personal data by fraudulent, unfair or unlawful means is punished by five years' imprisonment and a fine of €300,000*" (€1,500,000 when committed by a legal person).

When data collection lacks transparency, it is deemed unfair: for instance, collecting the personal email addresses of natural persons on the Internet without their knowing, as it goes against their right to object;[14] being able to mark teachers even though you are not one of their students;[15] or Facebook collecting data on the browsing activity on third-party websites of Internet users that are not registered on Facebook.[16]

The fairness of online platforms is now also understood in terms of transparency. The French Digital Law of 7 October 2016 requires online platforms (Facebook, Twitter, Airbnb, Uber…) to "*deliver loyal, clear and transparent information, especially on the methods of referencing*".[17] It also introduces ***trusted digital third parties***, which in this case are organisations certified by the French Data Authority (CNIL), responsible for handling, at their re-

13 See in particular Art. 8§2 of the Charter of Fundamental Rights of the European Union and Art. 5§1 of the GDPR.

14 French Court of *Cassation*, Criminal Chamber, 14.03.2006, Appeal No 05-83.423.

15 Paris Court of Appeal, 25 June 2008, 08/04727, affaire « note2be ».

16 CNIL, Ruling No 2016-007, 26 January. 2016: "When users navigate on third-party website pages including a Facebook social plugin (i.e. a "Like" button), the company collects data on the browsing activity of Internet users not registered on the Facebook.com website [...]. While the purpose put forward by the company might seem legitimate (improving service security), the collection of data on the browsing activity on third-party websites of Internet users not registered on the Facebook.com website is carried out without their knowing." [Unofficial translation from the French].

17 Art. 49 of Act No 2016-1321 of 7 October 2016 for a Digital Republic, OJ of the French Republic of 8 October 2016.

quest, the data subject's "*instructions relating to the [storage, deletion and communication] of their personal data after their death.*"[18]

As it is rooted in social processes, law relies both on confidence and trust, thus shaping two intertwining trends that it seeks to regulate, as we now turn to explain.

2.2. Functions of trust

Trust is essentially the result of a social link that was built over time. As we just explained, it consists in having faith in someone, as trust leads people to interact more frequently and contributes to reducing uncertainty about the outcome of interactions (see Chapter 1). If others are not trustworthy or sincere, law intervenes so as to protect the weaker party and impose sanctions. Such protection reflects how society aims to create and ensure some kind of societal cohesion in tolerable conditions. To this end, law establishes certain obligations and represses certain behaviours so as to provide a guarantee that society will function in a minimally viable way, thus contributing to building confidence.

On another level, law also aims to ensure that the economy runs smoothly. When law aims to regulate a market with free movement, especially the free movement of data in the digital environment, lawmakers seek to reach trust not on the weaker party's part, but on the consumer's. Protecting consumers is indeed a prerequisite for them to "accept" the information society, as it has now become "*a digital economy, a so-called social perspective that has given way to economic requirements, yet that also includes social aspects.*"[19]

The tension between the aim to ensure the market is running properly and the need to make rules that benefit consumers is clear from the very title of the GDPR, a regulation "on the protection of natural persons with regard to the processing of personal data and on the free movement of such data." The European Commission also highlighted that in its 2012 Communication called "Safeguarding Privacy in a Connected World."

---

18 Art. 40-I of Act No 78-17 of 6 January 1978 on Data Processing, Files and Individual Liberties, amended by Art. 63 of the French Digital Republic Act, aforementioned.

19 Agosti, P., Caprioli, E.A., (2005). *La confiance dans l'économie numérique (Commentaires de certains aspects de la loi pour la confiance dans l'économie numérique) (LCEN), Petites affiches*, 03/06/2005, n°110, p. 4. [Unofficial translation from the French].

« Lack of confidence makes consumers hesitant to buy online and accept new services. Therefore, a high level of data protection is also crucial to enhance trust in online services and to fulfil the potential of the digital economy, thereby encouraging economic growth and the competitiveness of EU industries.»[20]

The aim is therefore to create trust in the market — as opposed to confidence, since the term "trust" is used in recital 7 of the GDPR.[21]

Other evidence of such intertwining trends includes the evolution of the legal bases of legislation. Directive 95/46/EC on Personal Data, adopted in 1995,[22] is legally based on Article 100a of the Treaty establishing the European Community on the approximation of the provisions laid down by law which have as their object the establishing and functioning of the internal market. The GDPR, adopted in 2016, has for legal bases Article 8(1) of the Charter of Fundamental Rights of the European Union and Article 16(1) of the Treaty on the Functioning of the European Union, which both provide that "*everyone has the right to the protection of personal data concerning them.*"

This can be interpreted either as market mechanisms having a grip on a field that initially fell within the competence of law or, conversely, as a reconciliation of protecting the weaker party (the data subject) with the free movement of information in order to boost economic growth and business competition.

However, a shift in the relative powers of social link and commercial exchanges seems to be taking place, as consumer protection is becoming increasingly important. For instance, the French Digital Republic Act of 7 October 2016 introduced a new section under the Consumer Code (Article L. 224-42-2), which grants the consumer the right "to recover all of his data." This article however also specifies that "*such recovery of data shall comply with the provisions of Article 20 of the [GDPR] as regards data of a personal nature.*" Then,

---

20 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Safeguarding Privacy in a Connected World - A European Data Protection Framework for the 21st Century, COM/2012/9 final, Brussels, 25.1.2012, p. 2.

21 Which states that "*those developments require a strong and more coherent data protection framework in the Union, backed by strong enforcement, given the importance of creating the trust that will allow the digital economy to develop across the internal market.*"

22 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, ECOJ, L. 281, 23.11.1995, p. 31.

why was the right to portability not directly included in the French Data Protection Act (*loi Informatique et Libertés*)? The main purpose here is to "*reduce market stickiness.*"[23] This clearly belongs to risk management practices, as such rules are meant to reduce uncertainty and empower people to make their own decisions with full knowledge of the facts. The revised Article 1 of the French Data Protection Act, introduced by Article 54 of the Digital Republic Act, exemplifies this perfectly: from now on, "*all data subjects have the right to decide on and control the use made of their personal data.*"

Such right to decide is meant to empower citizens by giving them greater agency and control, especially by compelling other parties to provide greater information and transparency. Deciding how personal data should be used would therefore fall to the data subject, no longer to lawmakers or the Data Protection Authority. These changes raise several questions, as the focus is now much more on trust, in its most individual form, than on confidence. According to Nicolas Ochoa, Data Protection Expert, "*giving data subjects more power actually means depriving them even more in their unbalanced relationship with increasingly powerful data controllers. [...] Such principle comes down to knowingly manipulate everyone's weak free will when it comes to extremely technical issues, for which non-specialist individuals, given the important technical aspect, should be considered protected adults for their own good.*"[24]

Similarly, one may wonder what the reasons are behind this switch from a system where the supervisory authority allows data processing, as implemented by the 1978 French Data Protection Act, to one that focuses on consent on the part of GDPR subjects. Do individuals really exercise their free will when they consent to any use of their personal data, i.e. when they click to agree to a website's terms and conditions, knowing that refusing will prevent them from accessing the website? Ochoa points out that "*given the strong growth of the digital economy and its massive and increasing reliance on personal data, this makes sense*" and fits the main purpose of increasing data flows.

---

23 Government Bill for a Digital Republic recorded by the Office of the Presidency of the National Assembly on 9 December 2015, *Projet de loi pour une République numérique enregistré à la Présidence de l'Assemblée nationale le 9 décembre 2015*, 14th term, No 3318.

24 Nicolas Ochoa, « *La libre disposition des données personnelles : retour sur un braquage discret des droits et libertés* », 27/01/2016, https://www.lesechos.fr/idees-debats/cercle/cercle-147345-la-libre-dispositiondes-donnees-personnelles-retour-sur-un-braquage-discret-des-droits-et-libertes-1195601.php [Unofficial translation from the French].

2.3. Intertwining hard and soft law to implement trust

This aspiration towards the free movement of data is taking place while the legal scene itself is being deeply reorganised.

Indeed, rules of law are not merely binding anymore; they also aim to nudge behaviours. Seals play a special part in such context, as outward and visible signs of trust.

Law is traditionally defined as a set of standards established by public authorities and subject to sanctions for non-compliance. Such traditional conception, as taught by jurist Hans Kelsen, is called "hard" law and is symbolised by bindingness, public authorities and sanctions. It is nowadays increasingly being passed on by what is called "soft" law.

Soft law refers to a set of non-binding rules established by public or private entities, exempt from sanctions if not complied with. Soft law calls for a new definition of standards; and as such is criticised by supporters of the Rousseau conception of the rule of law, which they consider should have a legal binding force. Unlike hard law, soft law "*encourages rather than binds, suggests rather than imposes, guides rather than compels.*"[25] In 2013, in its annual study, the French Council of State (*Conseil d'État*) defined it as "*a set of instruments that meet three cumulative requirements:*

- *They aim to change or nudge citizens' behaviours by seeking, when possible, their support;*
- *They do not themselves create rights or obligations for citizens;*
- *Their contents and creation process are somewhat formalised and structured, which makes them similar to rules of law."*[26]

Examples include opinions and guidelines, including WP29's;[27] CNIL recommendations and compliance packages; codes of conduct; ethical principles; Binding Corporate Rules – that allow multinational corporations to create rules applicable to all their branches –;

25 Mekki, M., (2009). *Propos introductifs sur le droit souple*, *in Le droit souple, Dalloz, Coll. « Thèmes et commentaires »*, 2009, p. 11.

26 Council of State report on soft law. *Conseil d'État, Le droit souple, Les rapports du Conseil d'État, La documentation française*, 2013, p. 61, http://www.ladocumentationfrancaise.fr/rapports-publics/144000280/index.shtml. [Unofficial translation from the French].

27 WP29 (Article 29 Data Protection Working Party)

technical standards. These are all heterogeneous instruments that have a certain degree of normative authority. Such authority is not binding yet encourages behaving in a certain way.

Since they are non-binding, soft law instruments are somewhere along the spectrum of the normative chain between strictly binding law to soft law. Therefore, it often happens that hard law texts provide for the existence of such instruments, and sometimes even grant them a part in defining their rules of enforcement.

► Data protection certification, seals and marks are a good example of soft law. The GDPR recognises these instruments as a way to achieve compliance with the principles of accountability as well as adequacy in the case of international data flows (see Chapter 8). Entities that use them are granted some kind of advantage, since they are exempt from providing further justification.

Supporters of soft law emphasise its flexibility, arguing it can be useful at the international level while helping to address emerging and quickly evolving phenomena (especially technological changes,[28] by exploring potential fields, such as IA and drones) and preparing new binding texts. Its opponents however point to the way soft law bypasses democratic institutions and undermines qualities that are required from law, such as the clarity and stability of the standards defined. In a 1991 report, the French Council of State expressed concern that the principle of legal certainty was being threatened by an unprecedented inflation of standards, and famously stated that "*inflation means devaluation; when the law chitchats, citizens hardly listen.*"[29] The chitchat that the Council was denouncing is "lax" law, or law in the "gaseous state" — which qualities the Council ended up praising in 2013.

Soft law has become an important part of data protection regulation. As the CNIL President Isabelle Falque-Pierrotin explains: "*beyond prescriptive regulation, there is a need for partnership-based regulation, based on tailored legal instruments,*"[30] which is why the CNIL intends to favour dialogue and actor empowerment. Seals are thus an imple-

28 See also *Le droit souple, Rapport du Conseil d'État*, aforementioned, p. 91.

29 *Conseil d'État, De la sécurité juridique, Rapport public annuel 1991, La documentation française*.

30 Isabelle Falque-Pierrotin, « *Le droit souple vu de la CNIL : un droit relais nécessaire à la crédibilité de la régulation des données personnelles* », in *Le droit souple, Rapport du Conseil d'État*, aforementioned, p. 241.

menting tool, supporting data protection principles established by hard law and are meant to define best practices and contribute to solving operational issues. One can only notice how much this tool, which is downstream of the hard law and seems to be an outward sign of trust, is now increasingly being used.

2.4. Seals are outward signs of trust

Seals are not officially defined in French Law. The CNIL does not provide a technical definition for seals either yet describes them as a measure of consumer trust. Abstractly speaking, the doctrine considers seals as "*a way of recognising of a certain quality level, issued by a private entity or a public authority, backed by a benchmark (criteria).*"[31,32]

In concrete terms, seals have different uses in various fields, such as the environment and the food-processing industry. Article L. 115-22 of the French Consumer Code provides that "*Agricultural labels attest to the fact that a foodstuff or a non-food, unprocessed agricultural product possesses a distinct set of qualities and specific characteristics which have been fixed beforehand in specifications and establishing a superior level of quality… This product must be different from similar products of the type usually sold, in particular, in respect of its special production or manufacturing conditions and, possibly, in respect of its geographical origin.*"

Seals rely on companies' voluntary action. Indeed, seals are not compulsory and therefore belong to soft law. However, even though choosing to certify indicates a degree of free will, seals are still binding in the sense they may imply sanctions, even though these are not fines. Withdrawing a seal may be viewed as a moral sanction harmful to the company's image.

Seals are different from certification which, according to Article L. 115-27 of the Consumer Code, is the "*certification of a product or service subject to the provisions of this section is constituted by the activity by which an organisation, independent of the manufacturer, the importer, the supplier or the service provider attests, at the latter's request and carried out*

31 Naftaski, F., Desgens-Pasanau, G., (2010). *Enjeux et perspectives du pouvoir de labellisation de la CNIL, Revue Lamy Droit de l'Immatériel 2010*, n°63.

32 In French, the CNIL uses the term "*référentiel*" (benchmark in English), whereas the notion of criteria is widely used in English.

for commercial ends, to the fact that a product or a service conforms to the characteristics described in a benchmark and being subject to checks. The benchmark is a technical document defining the characteristics that a product or a service must display and procedures for checking conformity of the product or service to these characteristics."[33] It should be noted that public authorities still play a part in the process; even though some seem to think that certification is being "privatised."[34] At the international level, the International Organization for Standardization (ISO) defines certification in a similar way, as "*the provision by an independent body of written assurance (a certificate) that the product, service or system in question meets specific requirements.*"[35]

Certification is an either voluntary or mandatory process that is based on criteria established by a recognised organisation and is carried out by accredited auditors who are unrelated to applicants. However, these criteria are not necessarily equivalent to legal obligations. Successful assessment processes lead to the issuance of official certificates of compliance with a set of criteria. The final result indicating that certification has been obtained may take many forms: seals, marks or certificates.

Besides, companies may be certified without actually holding a label or a mark: certification is either mandatory, or merely allows organisations to assess their internal functioning in order to improve their processes.

Health data and online gambling are good examples of mandatory certification in France:

- nowadays, hosts of health data have to be accredited by order of the Minister for Health, further to approval from the CNIL and the Accreditation Committee of Hosts (*Comité d'Agrément des Hébergeurs* — CAH). Accreditation is granted for a three-year period.[36] 96 health data hosts have been accredited so far. As of 2018, it will

33 Law No. 94-442 of 3 June 1994, amending the Consumer Code with regard to the certification of industrial products and services and the marketing of certain products, published in the OJ of the French Republic of 4 June 1994.

34 Pontier, J.-M., (1996). *La certification, outil de la modernité normative*, D. 1996, p. 355.

35 https://www.iso.org/certification.html

36 Art. L. 1111-8 of the Code of Public Health inserted by Law No. 2002-303 of 4 March 2002 on patients' rights and the quality of the health system, published in the OJ of the French Republic of 5 March 2002, and Art. R. 1111-10 inserted by Decree No 2006-6 of 4 January 2006 on the hosting of personal healthcare data and amending the Code of Public Health (regulatory provisions), published in the OJ of the French Republic of 5 January 2006.

be compulsory for hosts of health data in digital format to hold a compliance certificate,[37] delivered by an accredited certification organisation of their choice, among the French accreditation authority, COFRAC, or the EU authority.[38]

- similarly, gambling operators are required to get accreditation from the French Online Gaming Regulation Authority (*Autorité de Régulation des jeux en ligne* — ARJEL). Certification is mandatory and is issued by certification organisations.[39]

All three terms "seal", "certification" and "mark" are used in the data protection field. The French Data Protection Act provides that the CNIL "*shall deliver a privacy seal to products or procedures.*"[40] "Seal" is also used by private organisations, such as ePrivacy consult GmbH's ePrivacy Seal in Germany, the EU eSafety Seal, and the Better Business Bureau (BBB)'s Accredited Business Seal for the Web in the United States. In the United Kingdom, the Information Commissioner Office (ICO) is considering issuing Privacy Seals, which it defines as "*stamps of approval that demonstrate good privacy practice and high data protection compliance standard.*"[41] At the EU level, the European Privacy Seal, called EuroPriSe, provides compliance certification.[42]

The development of data protection seals therefore draws much of its inspiration from certification procedures. In Germany, for instance, environmental audit procedures drawn up in the 1990s were used as models to develop data protection seals that are now mostly supplied by private actors. In the environmental sector as well, seals rely on certification for delivery.

---

37 *ASIP Santé, Évolution de la procédure d'agrément des hébergeurs de données de santé*, http://esante.gouv.fr/en/services/referentiels/securite/le-referentiel-de-constitution-des-dossiers-de-demande-d-agrementdes.

38 Order No 2017-27 of 12 January 2017 on the hosting of health data, amending Art. L. 1111-8 of the Code of Public Health, published in the OJ of the French Republic of 13 January 2017.

39 In particular, see Part V "*Informations relatives aux comptes joueurs*" of Annex II of the Regulation on certification, as provided for by Article 23 of Law No. 2010-476 of 12 May 2010 on opening the online gambling and betting market to competition and regulation, adopted by ARJEL Board Decision No. 2014-018 dated17 March 2014, amended by ARJEL Board Decision No. 2016-006 dated 18 February 2016, http://www.arjel.fr/IMG/rc/certification2.pdf (French text only).

40 Art. 11-3) c) of the French Data Protection Act, aforementioned.

41 See https://ico.org.uk/for-organisations/resources-and-support/privacy-seals/.

42 Offers certification to compliant […] products, […] services and […] processings, see https://www.europeanprivacy-seal.eu/EPS-en/Home.

In France, the CNIL delivers "Privacy Seals", yet the Act for a Digital Republic of 7 October 2016 also allows it to publish "*criteria for the purpose of certifying compliance of [data protection] anonymisation processes*". Switzerland, for its part, adopted an ordinance on data protection certification on 28 September 2007.

Private actors also use the term "certification":

- in Spain, the Professional Association for Privacy (*Asociación Profesional Española de Privacidad* – APEP) issues the APEP-Certified Privacy certification;
- Germany provides several certifications, including TÜV Rheinland's Data Privacy Certification for Companies and *Gesellschaft für Datenschutz und Datensicherheit* (GDD)'s *Zertifizierung der Datenschutzqualifikation*;
- in Italy, TÜV Italia/TÜV SUD GROUP provides the *Certificazione di privacy officer e consulente della privacy*;
- at the EU level, the European Interactive Digital Advertising Alliance (EDAA) issues the OBA Certification.

Trust marks mostly operate in the trade sector and are issued by associations, including:

- in France, the FEVAD trust mark, issued by the *Fédération du e-commerce et de la vente à distance* (FEVAD);
- in Austria, TrustMark Austria, issued by the Handelsverband association;
- in the EU, the Ecommerce Europe Trustmark, issued by the Ecommerce association.

Data protection seals are therefore framed as the final result of a written certification. As the outward signs of a voluntary process, they rely on criteria defining certain legal obligations. The kind of trust that is sought here is therefore defined in relation to other notions, including fairness, security and responsibility. It lies at the ambiguous crossroads between the protection of users and the free movement of personal data, which is allegedly crucial to developing the digital economy.

How to cite this chapter: Levallois-Barth C. “Trust as embraced by law”, *in Signs of trust – The impact of seals on personal data management*, Paris, Handbook 2 Chair Values and Policies of Personal Information, Coordinated by Claire Levallois-Barth, January, 2018, chapter 2, pages 21–35.

http://www.personal-information.org/

Chapter 3. The notion of trust in economics

Patrick Waelbroeck
Antoine Dubus

3

The notion of trust in economics can be initially approached as a reduction of the risks related to transaction. The barometer of trust of the ACSEL-CDC never uses the word trust directly, but asks questions about the risks associated with online information sharing and economic transactions. One way to understand the notion of trust is to analyse the factors that reduce those risks. Knowledge that helps better distinguish the states of nature[1] and build better economic models can reduce uncertainty and risk.

Two basic economic mechanisms improve trust. The first one is knowledge; the second one deals with the notions of fairness and reciprocity. We first examine the different notions of risks associated with a transaction (3.1). We then show how short-term strategies can become counterproductive when trying to build long-term cooperative equilibria where interactions are repeated (3.2). It is also an opportunity to highlight the role of punitive mechanisms in building trust. We then discuss situations in which consumers reduce uncertainty and punish bad business practices by participating to a collaborative reputation system (3.3).

We then present the second pillar of trust studied in numerous experimental economic studies dealing with the concept of fairness (3.4). We argue that digitization is weakening both pillars of trust by reducing knowledge sharing and reciprocity in the face of asymmetries

1 The states of nature are defined as the different probabilistic outcomes resulting from an economic activity, for example the cost of producing a good, or the level of computer security of an online service provider. Economic agents do not necessarily know these states.

The notion of trust in economics

of power and of information (3.5). We finally discuss how privacy and data protection labels can act as signals of trustworthiness (3.6).

3.1. Trust as a subjective means of reducing risks

Uncertainties involve risks that are largely studied in economics: systemic risk, idiosyncratic risk (specific to a particular situation), strategic risk... We can group risks into three broad categories. The first category corresponds to ***probabilistic risks***, for which it is possible to make calculations of expected utility, according to the different probabilities that one grants to the states of the nature. The second category of risks is *non-probabilistic*. These risks are related to the notion of ***uncertainty*** (corresponding to situations where agents cannot formulate probabilities when certain events occur). The third category concerns the notion of ***incompleteness***, which corresponds to a situation where an economic agent does not know or fails to distinguish the different states of nature.

Probabilistic risk makes it possible to understand the notion of trust through learning related to signals or repeated interactions. Bayesian learning, for example, combines a prior distribution and a likelihood function to form a posterior distribution. This learning through signal observation reduces risks and increases trust in the transaction. This approach is necessarily subjective since prior distributions may depend on factors that vary greatly from one individual to another. In addition, the way in which risk is taken into account also varies among economic agents. We are talking about different forms of risk aversion, or

loss aversion, because individuals do not respond symmetrically to risks related to gains and those related to losses.

The second category makes it possible to refine these asymmetric behaviours in risk perception through non-expected utility theory, which takes into account reasonings which go beyond the average (the average is not enough as a risk assessment criterion) while accepting the idea that some risks are subjective.[2]

The third type of risks relates to the incompleteness of the states of nature and is closely linked to the notion of knowledge, because this type of risk depends on what an agent knows about all the possible events. Let us take an example: a patient goes to see his doctor. He describes symptoms that make him think that he is sick, but does not know the disease he is suffering from. So, he can distinguish at this stage two states of nature: *to be in good health* or *to be sick*. The doctor examines him and informs him that his symptoms may correspond to two diseases. After consulting the doctor, the patient now knows three states of nature: *to be in good health*, *to suffer from disease1*, *to suffer from disease2*.

3.2. Repeated interactions and punitive mechanisms

Risks can be reduced by using a punitive mechanism, as we will argue later on using the example of tacit agreements in repeated games. We also trust others because we know that the system makes it possible to correct or punish agents who behave badly. If you know the terms of the transaction better, you can create trust between the parties involved in the transaction. The best way to illustrate this is to consider the economic equilibria change when one moves from equilibria in one-shot game to equilibria with infinitely repeated interactions. The ***prisoner's dilemma*** considers a situation where two accomplices of a wrongdoing are questioned separately by the police. If both prisoners do not denounce each other, they are sentenced to a minimum penalty. If both cooperate with the police, they both serve a maximum sentence. If one cooperates and the other does not, the first enjoys a favourable treatment and the second serves a heavy sentence. The best situation for the two accomplices is not to cooperate with the police and to trust each other. However, one of the two accomplices always has an incentive to deviate from this

2 See Machina, M., (2007). Non-expected Utility, *in Darity (Ed), International Encyclopedia of the Social Sciences*, Macmilan Reference USA, 2nd Edition.

situation and to denounce his accomplice in order to lighten his sentence, so that the only equilibrium is a situation in which the two accomplices denounce each other.

The fact that this situation occurs only once is crucial to understand this equilibrium of distrust. If we repeat this situation an infinite number of times, it turns out that cooperative equilibria emerge, where economic agents trust each other.

In ***tacit collusion models***, several companies compete over several periods. Contrary to the prisoner's dilemma, as long as the time discount factor (which makes it possible to convert tomorrow's euros into today's euros) is relatively low, an equilibrium with a tacit agreement — where companies do not communicate directly and nevertheless cooperate— emerges. The reason is the following: when an agent decides to deviate unilaterally, the other agents can punish him so that the gain from the unilateral short-term deviation is not profitable compared to the gains of a long-lasting collaboration. This ***punishment*** mechanism is crucial to understand the emergence of this equilibrium of trust.

3.3. Reputation systems and trust

Reputation systems are another way to build trust. Reputation is defined as "*goodwill*",[3] that is, a stock that increases with positive experiences. Many articles in the economics literature specifically study the eBay platform given its well-known rating system. These studies clearly establish the existence of a reputation premium: a reputable seller can sell at a price above the market price. Bounie et al. (2012) find that the reputation premium on Amazon Marketplace can reach 10%. Reputation also has an effect on the probability of performing a transaction (for a seller). For example, Cabral and Hortacsu (2010)[4] find that a one percent increase in the number of negative evaluations leads to a 7.5% decrease of the price of a seller. They also show that when a seller receives his first negative rating, his sales decrease by 13%. A seller who receives multiple negative ratings is more likely to

3 The *goodwill* account can be found in the assets portion of a company's balance sheet and represents the difference between the price of an acquisition and the value of the real assets. Know-how, R&D projects, social climate, brand value and reputation are among the elements taken into account to establish it.

4 Cabral, L, Hortascu, A. (2010). Dynamics of Seller Reputation : Theory and Evidence from eBay, Journal of Industrial Economics, v. 58, no.1, March 2010, pp. 54-78.

leave the online platform. Thus, the active management of one's reputation profile has an economic value and explains why people are trying to look their best online.

3.4. Trust through fairness and reciprocity

Repeated interactions also create trust through reciprocity and fairness. These concepts are analysed in the experimental economics literature that focuses on variants of the dictator game. In the dictator game (which is actually not a game because there is only one person who chooses his/her strategy), the dictator determines how to divide an amount, say 10 €, between him/her and an anonymous beneficiary. The outcomes of the experimental studies show that a large number of dictators choose a fair distribution — each participant receives a comparable amount —, whereas individual rationality without pro-social concern should have led the dictator to keep everything for himself/herself. The knowledge of the identity and of the socio-economic profile of players is important: the closer the social proximity is, the fairer is the income distribution.

The trust game is a variant of the dictator game where the amount given by the dictator to the beneficiary is multiplied by an arbitrary number, for example doubled; the beneficiary can give back all or part of the amount received. Again, the experiments show that the beneficiary returns a non-zero amount corresponding to a reciprocal behaviour. We understand that we must both *trust* and be *trustworthy*.

3.5. Impact of digitization: reducing knowledge externalities and social cohesion; increasing asymmetric information

In addition to building trust, knowledge sharing enables economic development and innovation. Growth models show how long-term economic growth depends on how knowledge accumulates and spreads in the economy. These models assume that entrepreneurs and innovators contribute to the stock of knowledge of the economy from which other present and future innovators can find the necessary techniques to design new products and services. This intertemporal knowledge externality is the engine of long-term growth, because future entrepreneurs draw their inspiration from today's knowledge. It is interesting to note that a patent is granted to an inventor in exchange for the disclosure of the technical process underlying the invention, contrary to innovations protected by secret. In

general, human exchanges of knowledge generate externalities through social exchanges (for example “word of mouth” or reputation systems).

Paradoxically, while we live in a knowledge society, these exchanges of knowledge are threatened by automation, by the secret of algorithms and by predictive algorithms. First, automation related to the use of robots and algorithms reduces human intervention in production processes and decreases the knowledge of workers and craftsmen (see articles by Bernard Stiegler[5] for example on this point). Moreover, some acquired skills are not easily encodable, that is, they are difficult to describe by a sequence of procedures or an algorithm (for example, the sophisticated gestures of a craftsman such as a cabinetmaker or a luthier). We are talking about tacit knowledge that is also lost through automation. Secondly, many innovations related to Big Data and algorithms are currently kept secret by companies, so the mechanism described in the previous paragraph is neither operational nor verifiable. Thirdly, predictive algorithms can lead, through their encoded and deterministic targeting, to lock Internet users into filter bubbles. Independently of whether it is the algorithm that locks up or if it is the individual who locks himself/herself by his/her behaviours or choices, the result is identical: he/she may be find it hard to share information with other Internet users that engenders trust in the online community. Thus, in the media sector, there is a risk of an algorithmic polarization of opinions that can clearly undermine the foundations of the democratic society as we know it.

3.6. The role of labels in economics

Digital technology disrupts the conditions of exchange by generating asymmetric information, a situation that F. Pasquale calls the *black box society*:[6] the users of digital tools do not know how their personal data are being used, nor the volume of data exchanged by the companies that collect them. Worse still, these companies can manipulate the information context of the transaction to put people in an environment they believe to be trust-

5 Stiegler, B. (2015). *La Société automatique. L’avenir du travail*, Fayard

6 Pasquale, F. (2015). The Black Box Society: The Secret Algorithms That Control Money and Information, Harvard University Press

worthy (see the articles of Acquisti[7]) in order to encourage them to disclose more personal information.

Asymmetric information weakens fairness and reciprocity in the transaction and creates a feeling of helplessness for isolated Internet users facing large Internet companies (what sociologists call informational capitalism).

Labels and trust marks are signals that allow users to better understand the risks of the transaction in order to solve the informational problems discussed above.

These labels and other signs of trustworthiness are analysed in the economics literature by signal theory. This theory seeks to solve asymmetric information issues through a costly signal that consumers can interpret as a pledge to good practice. Thus, the costlier the signal, the greater the impact, provided of course that consumers are aware of its cost. If the label is essential in an uncertain environment in a short-term relationship, the brand on the contrary is more sustainable in the long run. The brand act as a reputational mechanism in repeated interactions leading to *goodwill* on the part of consumers. Thus, labels and brands appear, in economics at least, as substitutable or at least emerging in different timeframes.

7 Acquisti, A. (2012). Nudging Privacy: The Behavioral Economics of Personal Information. *in Jacques Bus, Malcolm Crompton, Mireille Hildebrandt, George Metakides (eds)*, Digital Enlightenment Yearbook 2012, IOS Press

How to cite this chapter: Waelbroeck P., Dubus A. “The notion of trust in economics”, *in Signs of trust – The impact of seals on personal data management*, Paris, Handbook 2 Chair Values and Policies of Personal Information, Coordinated by Claire Levallois-Barth, January, 2018, chapter 3, pages 37–44.

http://www.personal-information.org/

« Le Conciliabule » –Thierry Citron

Chapter 4.

Building trust through risk management in computer science

Maryline Laurent
Armen Khatchatourov

4

Trust in computer science mostly relies on evaluating the risks of using a tool (software or hardware) or, more generally, any other form of digital service (i.e. a website). This evaluation and its reliability are all the more critical as stakes get higher: they are most important when dealing with an organisation's Information Systems Security (ISS).[1]

There are two main approaches to risk qualification. The older method regards products delivering ISS (software and hardware) and implementing security functions, and trust service providers (e.g. providing timestamps, signatures, electronic certificates). Often, public authorities are involved in the process of qualifying the level of risk. Here, trust is assumed to be transitive: if users trust the qualifying entity or the electronic certificate, they will also trust the object that is qualified. Qualifying products or providers is not always mandatory, but it is unavoidable when designing critical security solutions or competing for public procurement, among other cases. Therefore, such risk management approach is, together with the reliability level it is associated with, an external sign aiming to reinforce the trust of individuals and companies (4.1.).

The second and more recent approach relies on the large and growing number of data points available in IT system. It works by scoring the security performance of individuals and services. This score, used as a risk indicator, is based on a behavioural analysis that

1 In this chapter, "Information Systems Security" refers to all the technical, organisational, legal and human processes in place to ensure the protection of an organisation's IT system.

Building trust through risk management in computer science

benchmarks one behaviour with a reference behaviour. It is likely to have a direct influence on trust (4.2.).

These approaches – product and provider qualification and behavioural analysis — can be used jointly, for instance in order to authenticate a user based both on an electronic certificate and on their behaviour.

4.1. Risk evaluation of ISS products and services

Security is fundamental for States and companies

The evaluation of the risk associated with using ISS products and services has historically been tied with the strong need for companies and States to keep providing trusted and available infrastructure and services and fight cybersecurity threats. Designed in a top-down way, risk evaluations take place in a strict framework laid down by national and/or European authorities. This framework regulates the reliability level expected from services, hardware and software contributing to the security of information systems — each level is associated with a level of qualification. The goal here is to maintain a high level of vigilance, the stakes being all at once economic, political and strategic. Therefore, in order to ensure national sovereignty, States qualify ISS products and trust services likely to be used by their administration, critical infrastructure providers or otherwise sensitive companies. The highest level of qualification corresponds to low risk-taking and is therefore adapted to critical infrastructures.

None of these qualifications are mandatory, yet they are difficult to avoid in practice. In particular, they make it easier, through a sort of nested doll effect, to obtain data protection seals, as they guarantee that confidentiality and security requirements are taken into account. Besides, certain regulations are compulsory, notably those regarding the provision, import, export, or transfer of cryptological tools associated with a product or service towards another EU country.

In this context, public authorities — in France, the National Agency for the Security of Information Systems (ANSSI in French) — publish a catalogue of qualified products that includes the level of qualification obtained and the list of qualified trust service providers. This does not provide absolute guarantee — indeed, recent events have shown that certain security products included backdoors or purposefully deteriorated security functions so that data flows could be decrypted with no prior knowledge of secrets. In 2013, Reuters therefore revealed[2] that the National Security Agency (NSA) had paid a $10 million bribe to RSA so that it would implement by default a weak random number generator called Dual EC DRBG (Dual Elliptic Curve Deterministic Random Bit Generator) in their security product BSAFE, in order to enable rapid decryption of the data of millions of users. Besides, it seems the NSA also originated a modification of the Dual EC DRBG algorithm officially meant to enhance the security of the encrypted data; yet, as researchers have shown, the modification actually reinforced vulnerabilities.

ANSSI-issued qualifications for products

In France, ANSSI, within the Secretariat-General for National Defence and Security (SGDSN in French) under the Prime Minister's Office, developed its own certification scheme for information systems security products on the basis of a co-regulating scheme (see Chapter 5, "Numerous and heterogeneous seals…", page 64): the qualification is issued by ANSSI while the evaluation is carried out by private evaluation centres accredited by ANSSI. Depending on the products and levels of reliability, qualifications are issued based on audit or technical test results.

Three levels of qualification are issued[3] (see Table 1):

2 https://www.schneier.com/blog/archives/2007/11/the_strange_sto.html

3 Chochois, M., Magnin, N., (2015). *Qualité des produits de SSI, les labels français, Techniques de l'ingénieur,* H5825 v2, October 2015.

Object		Title	Benchmark	Number of qualified solutions	Duration of qualification
Products		Elementary qualification	ANSSI	70+	Unlimited for a given version
		Standard qualification	Common criteria EAL3+	30+	6 months
		Strong qualification	Common criteria EAL4+	70+	
Trust service providers	SecNum Cloud	Simple, advanced or qualified qualification depending on the type of service, *see "Identités numériques", Cahier n°1, Chair Values and Policies of Personal Information*	ANSSI	0	Up to 3 years
	PSCE			240+	
	PRIS			0	
	PDIS			0	
	PASSI			26	
	PSHE			240+	

Table 1. Security qualifications issued by ANSSI for products and trust service providers

SecNumCloud: Cloud Service Provider; PSCE: Electronic Certification Service Provider; PRIS: Security Incident Response Service Provider; PDIS: Security Incident Detection Service Provider; PASSI: Information Systems Security Audit Provider; PSHE: Timestamping Service Provider.

- **Elementary qualification** corresponds to a first-level seal for the ISS product, issued with limited time and resources. After ANSSI studies the file, an evaluation centre that has been accredited by ANSSI for First Level Security Certificates (CSPN in French) implements the CSPN certification scheme. Verifications include compliance of the product with its security specifications and the threats it protects against.

- **Standard qualification** requires more time and resources and guarantees the product for the treatment of sensitive unclassified information. The product is evaluated by the Centre for Evaluation of the Security of Information Technology (CESTI in French), also accredited by ANSSI. The evaluation relies on a benchmark with common criteria (see next section) under control of ANSSI. Standard qualification is granted for six months and requires the product to obtain at least the EAL3+ level determined by the common criteria. To this end, the manufacturer needs to provide several inputs, including cryptographic mechanisms (protection of private keys, random number management, etc.).

- **Strong qualification** also lasts six months and relies on obtaining an EAL4+ level of the common criteria. French products with this level of qualification are granted "*Confidentiel Défense*" and/or "*Secret Défense*" clearance, which enables them to deal with classified information.

International mutual recognition

Two different types of international mutual recognition agreements enable State A to accept a qualification issued by State B.

The first relies on the Common Criteria Recognition Arrangement (CCRA), the most recent update of which was signed in 2014. 28 countries currently recognise as valid the qualification of a given ISS product issued by one of their certification authorities, in accordance with the common criteria framework: Australia, Austria, Canada, the Czech Republic, Denmark, Ethiopia, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Malaysia, the Netherlands, New Zealand, Norway, Pakistan, Qatar, South Korea, Singapore, Spain, Sweden, Turkey, the United Kingdom, and the United States.

The common criteria allow to certify a product through a certification level called Evaluation Assurance Level (EAL); EAL1 being the lowest score and EAL7 the highest. They are often used to mandate certification levels according to uses. For instance, a smart card used for interbank transactions needs to be certified with at least EAL4+.

Mutual recognition agreements include certain limits depending on the type of evaluation scheme implemented. For evaluations under the generic common criteria, mutual recognition used to apply up to EAL2. In 2014, CCRA relaxed this rule and defined collaborative Protection Profiles (cPP) with a specific evaluation scheme on top of common criteria. For evaluations carried out according to cPP, mutual recognition now stands up to EAL4.

A second type of agreement was signed in 1999 and updated in 2010: the European Mutual Recognition Agreement of the Senior Officials Group Information Systems Security (SOG-IS).1 This agreement established mutual recognition of the validity of certificates in several technical domains. By default, the recognition applied up to EAL4 as with the common criteria arrangement — certain domains such as “smartcards and similar devices” and “hardware devices with security boxes” can benefit from a mutual recognition up to EAL7. 11 countries are part of this agreement: Austria, Finland, France, Germany, Italy, the Netherlands, Norway, Poland, Spain, Sweden, and the United Kingdom. For each technical domain, the agreement specifies which countries are qualified participants and can issue high-level qualifications.

The qualification of trust service providers

While ANSSI’s interventions may sometimes seem to disregard end users’ daily issues, the situation is changing with the implementation on July 1, 2016 of EU Regulation 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS).[4]

The Regulation introduces a legal framework common to all EU Member States for electronic identification means and trust services: electronic signatures, electronic seals,

4 Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS Regulation), EUOJ L 257, 28.8.2014. Readers are encouraged to consult Levallois, C. (2016). *La réglementation mise en place par l’Union européenne en matière d’identification électronique et des services de confiance (règlement eIDAS). in « Identités numériques », Cahier n°1 de la Chaire Valeurs et Politiques des Informations Personnelles,* coordinated by Claire Levallois-Barth.

electronic timestamps, electronic documents, electronic registered delivery services and certificate services for website authentication. It requires transposition at the national level; in France, ANSSI is the responsible agency. ANSSI is currently establishing the eIDAS requirements and issuing accreditations to organisations responsible for evaluating compliance.[5] As anticipated in the eIDAS Regulation, ANSSI has defined 4 types of services it deems useful: cloud service providers, incident response service providers, incident detection service providers, and ISS audit providers.

However, although the eIDAS Regulation has established a certain level of harmonisation, including a common terminology for trust services, it also comes with some shortcomings and ambiguities relating to data protection and user privacy, specifically regarding tracking and surveillance abilities. On this topic, we refer the reader to Chapters 7, 8 and 9 of the first volume published by the **Chair Values and Policies of Personal Information on Digital Identities**.

4.2. New forms of risk analysis associated with services and users

Behavioural analysis

In computer science, behavioural analysis primarily aims at detecting intrusions in IT systems and risky behaviours. Initially, it relied on the creation of a "normal" behaviour model for the information system and required a long training period. Since then, technology and its use cases have evolved to focus on User Behaviour Analytics (UBA) and incorporate the latest advances in Big Data and Machine Learning.

Table 2 presents a snapshot of current trends in risk evaluation: individuals, services and platforms can all be the target of behavioural analyses, carried out either by a team of individuals (II.) or through automated algorithmic methods (III.). In order to identify the true purpose behind using behavioural analysis, it is necessary to know both the organisation

5 https://www.ssi.gouv.fr/administration/reglementation/confiance-numerique/le-reglement-eidas/documents-publies-par-lanssi/

setting the norm and the type of criteria that will characterise this norm. Such information allows to better identify the nature of IT risks, the type of trust, and to discuss potential abuses.

For instance, an analysis conducted by a set of individuals (II.) allows to score a service provided by individuals or companies, be it by Amazon or eBay for products, or by TripAdvisor for restaurants and hotels. The reliability associated with reputation gets higher with every score and comment left on such websites, since it becomes all the more difficult to compromise the scoring system by leaving either positive reviews on your own page or negative reviews on the pages of competitor services. These scoring systems have already had a major impact on consumer behaviours. According to a PhoCusWright study,1 83% of respondents state that reviews on TripAdvisor help them pick the "right" hotel. Even though the technical infrastructure is not sophisticated, designers intend to build a trust relationship between service providers and consumers by drawing up a risk indicator; however, this only ensures a level of trust that some would call "weak."

Behavioural analyses can also be automated by algorithms for better efficiency and accuracy (III.). They can target one individual in particular (III.1.). In such case, the analysis can be used to reinforce the authentication mechanism between this individual and the information system — in addition to password or hardware-based authentication, the distance between the individual's usual behaviour and their current behaviour is taken into account in the authentication process in order to limit risks. The usual behaviour is therefore taken as a benchmark, while the nature and size of the acceptable differences are set by the system administrator. The reliability associated with the behavioural analysis is based on the quality and size of the available data on the individual's behaviour within the system, and therefore on how precisely their behaviour can be quantified (geolocation, which applications are used when, from which terminals, …). It also depends on the algorithm's ability to detect any unusual behaviour. The tool should thus include personalised thresholds to avoid both wrongly accusing individuals (false positives) and not detecting identity fraud (false negatives).

The main purpose of automated individualised analysis can however be abused, especially to generalise control over people's behaviours (III.1.). Each individual could receive a score depending on their behaviour and from there advantages or penalties. For instance, China is working on a new "social credit scoring" system which is announced for 2020.

	Risk analysis associated with digital services	***Behavioural analysis: establishing a score for services/users***		
External sign	Digital certificates, qualified services	Scoring		
Evaluator	Certification organisation (I.)	Human (II.)	Algorithm (III.)	
Subject of evaluation	Hardware / Software / Digital services	Service provided	Individuals (III.1.)	Individuals / websites (III.2.)
Norm designer	European Commission / Institutions	Set of individuals	Government / Services	Institutions / Platforms
Volume of Data		Large datasets	Large datasets on individuals	Large set of individuals / websites
Forms of trust	EAL/eIDAS certification	Scoring	Profiling / Scoring	Profiling / Ranking
Trust in…	Certification organisation / Service provider	Operator / Platform / Government		
Proof of trust	ANSSI-issued list of qualified service providers and products	Number of evaluations	Algorithm and number of profiles	Algorithm
Purposes	Trust ++	Evaluation of a service	Authentication ++ / Surveillance	Cyber surveillance / Website ranking

Table 2. *Two approaches to risk management in computer science*

Chinese citizens would be “ranked” according to their actions, and the “riskiness” of their behaviours would be measured.

Finally, automated analysis can be used on large groups of individuals, platforms or websites (III.2.), with either commercial or political purposes here as well.

Scoring systems, most notably Google’s, rank popular websites according to keywords; Apple’s rank popular apps in the App Store. However, algorithms supposed to rank products, apps or websites according to their popularity are still very opaque in the way they work, which can make it difficult to prevent abuse. For instance, in exchange for $11,000, Taobao was able to consolidate its ranking in the top 10 mobile apps in the App Store.[6]

Automated analysis can also be used to support implementing legislation, such as the HADOPI2 law (Creation and Internet law) or the Intelligence Act in France. The Intelligence Act, passed in 2015 in the wake of the January 2015 terrorist attacks, entitles authorities to collect and process data related to internet connections (metadata) and defines the cases where such measures are allowed. This detection, which mainly aims at ensuring national security, preventing terrorist actions and defending France’s economic interests, may be automated by an algorithm that benchmarks user behaviours against pre-set “normal” behaviours.

Classically, we observe that behavioural analysis techniques are a double-edged sword. They can contribute to laudable objectives such as the overall security of the digital environment, but also to more problematic commercial or institutional ambitions.

6 https://recombu.com/mobile/article/manipulate-apple-app-store-rankings-for-money-in-china

4.3. Towards hybrid, distributed and privacy-preserving trust systems

In computer science, three solutions are currently being studied to limit security risks and data leaks and to increase trust in digital products and services.

- ***Hybrid approaches*** to reinforce the security of classic ISS solutions by using behaviour analysis methods. Improvements in Machine Learning and Big Data, together with the collection of data on a massive scale, have led to the increasing reliance of security services on behavioural analyses in order for them to define the behaviour of an individual or an information system and to be able to measure deviations. Banks, for instance, are implementing strong authentication mechanisms relying on usual strong cryptographic tools together with behavioural authentication including contextual data (geolocation, time of connections, IP addresses of the terminal, terminal fingerprinting)[7] and data about user-terminal interactions (browsing habits on a website, mouse movements, typing patterns). Future trends will dive deeper into these behaviours and be more specific about the risk levels incurred.

- More ***transparency*** and ***decentralised governance***. Blockchain-related solutions are heading in this direction. The first goal of blockchain is to provide a service administered by multiple authorities, instead of being centralised in the hands of a single one. The algorithm implementing the service is publicly accessible and readable, and can thus be interpreted by anybody; therefore, any change in the way the service functions or is governed needs to be approved by consensus of the participating authorities before it is implemented. The results are increased transparency, seemingly more stability, and the impression for users that have control over the service and actors, which results in higher levels of trust (see Chapter 11).

- A better ***protection of user privacy***. Technological solutions are being developed to guarantee both security and data protection. Among these solutions is anony-

7 The digital signature of a terminal (terminal fingerprinting) contains multiple pieces of information (OS version, screen resolution) which are meaningless on their own but the combination of which identifies a specific terminal amongst millions of others.

mous certification,[8] which aims to minimise the quantity of personal data collected by service providers while guaranteeing them strict access controls (that the users are not minors, that they are geographically located in a certain region, …). One can also mention ***homomorphic encryption***, which aims to delegate part of data processing to a third party without revealing unencrypted data, and ***secure multi-party computation***, which enables a group of participants to contribute to computing operations while hiding which operations are being carried out and the data on which the computation is being done. However, these solutions are still slow to develop in practice. They face technical obstacles, with high energy costs, and economic ones, with the lack of incentives to adopt other models than the exploitation of personal data.

If blockchain technologies, decentralised governance systems, and the work towards a better protection of privacy are indeed factors of trust, one interesting avenue for research would be to identify more precisely the technical solutions underpinning confidence-friendly environments. This topic of research is undoubtedly necessary, but also questions the intervention and the role of public authorities in this area.

8 Laurent, M., et Kaâniche, N. (2016). *Les preuves d'identités ou d'attributs préservant le pseudonymat ; in « Identités numériques », Cahier n°1 de la Chaire Valeurs et Politiques des Informations Personnelles,* coordinated by Claire Levallois-Barth.

How to cite this chapter: Laurent M., Khatchatourov A. “Building trust through risk management in computer science”, *in Signs of trust – The impact of seals on personal data management*, Paris, Handbook 2 Chair Values and Policies of Personal Information, Coordinated by Claire Levallois-Barth, January, 2018, chapter 4, pages 47–59.

http://www.personal-information.org/

The next four chapters introduce the key learnings we deduced from the hundred seals we listed at the French, European and American levels (see lists in Chapter 5). These external signs of trust mainly qualify the collection and use of personal data, either generally or in a sector-specific context, such as cloud computing or e-commerce.

- Specifically, Belgian seal BeCommerce on e-commerce certifies the security and quality of transactions, complaint procedures, the information given to customers and child protection while guaranteeing the protection of their clients' personal data.

We thought it was important to list seals that certify certain principles of data protection, such as signs of trust focusing on security (see Chapter 4 for a more comprehensive overview). Despite the common confusion surrounding the notions of "*data security*" and "*protection of personal data*", these two terms should be carefully distinguished.

Protection of personal data vs. data security

Security is but one component of data protection; it is certainly a key principle, yet one of many principles, such as those of purpose limitation, data storage period, legitimation, sensitive data protection, etc.[1] Security primarily creates obligations for the personal data controller and processor, i.e. taking appropriate technical and physical measures (encrypting data, managing access permission, etc.) to protect people's data and prevent any unauthorised processing. The right to the protection of personal data is understood in a larger scope as both a fundamental right and a human right guaranteed by many national and international acts, in particular the Charter of Fundamental Rights of the European Union.

1 Levallois, C. (2016). Identités numériques et gestion des données personnelles. *in « Identités numériques »*, *Cahier n°1*, **Chair on Values and Policies of Personal Information**, coordinated by Claire Levallois-Barth

To facilitate comparison, our study focuses on signs of trust issued in Member States of the European Union and addresses the case of Swiss seals, which are relevant as they rely on principles close to those of the GDPR.

► Besides, our study relies on more than twenty qualitative interviews conducted from October 2015 to September 2017 with representatives of French certifying or certified organisations, consultancies and law firms. All interviews are listed in the Appendices, page 218.

Generally speaking, we find that certification stands at a crossroads between two approaches. One seeks to encourage economic actors to report on their legal compliance through regulation and responsibilisation mechanisms in which public authorities are strongly involved. Just like seals issued by CNIL and EuroPriSe, such signs of trust address all principles related to the protection of personal data, in a context of overall compliance (see Chapter 6). The second perspective aims to involve economic actors in their own regulation process through a self-regulation approach. In a societal and digital context in constant evolution, certification is intended to complement traditional legal structures as part of a search for credibility and competitiveness that focuses on “quality” criteria (see Chapter 7).

Chapter 5.

A French, European and international overview of personal data protection certification

Claire Levallois-Barth
Delphine Chauvet

5

The hundred signs of trust listed in this handbook are either called “seals”, “certifications” or “marks.”[1] While there is a variety of heterogeneous external markers of trust issued by different types of entities (5.2.), their procedures have actually proven quite similar (5.2.).

5.1. Numerous and heterogeneous seals…

This handbook indexes around a hundred French, European and American seals, including 75 issued in Europe and 22 issued in North America (United States and Canada) and Japan. It appears that ***certification organisations keep creating different seals***. Some seals only exist over a short span of time while others seem to be pure hand-waving, making it difficult to draw a comprehensive overview of data protection seals.

1 See Chapter 2, Section “2.4. Seals are outward signs of trust”, page 32.

A French, European and international overview of personal data protection certification

The proliferation of seals is most likely due to the fact that various professions have the skills required to establish criteria on personal data and assess the consistency between the requirements set by a company applying for certification and its actual practices, among which consultants, specialised lawyers and legal experts, auditors working in the field of ISO certification, IT engineers specialised in data security and cloud computing, marketing and communication experts, and economists. Specialisation defines the nature of the trust mark provided, according to the profession's covered field and set goals.

However, we can still draw an overview based on characteristics such as the geographic scope, scope of application and nature of the data protection certification organisation.

Seals are mainly issued by German organisations

First of all, seals are geographically very unevenly distributed. Germany and the United States are the largest certification providers. Out of the 75 European seals we listed, there are:

1. 41 in Germany;
2. 9 in France, including 4 issued by the French Data Protection Authority, the CNIL;
3. 4 in Spain and Switzerland;
4. 3 in Italy and the Netherlands;
5. 2 in the United Kingdom;
6. 1 in Austria, Belgium, Denmark and Luxembourg;
7. 5 European-wide seals.

Besides, we also picked out 22 seals from outside of Europe (United States, Canada and Japan).

In Europe, Germany is the country that produces the highest number of seals (see list of seals in Table 4, page 68 and following), for both legal and cultural reasons. While Germany sets strict frameworks for privacy and data protection, for historical reasons mainly, that number is also the result of the federal state's legal structure. Indeed, each Land can enact its own data protection act. For instance, the State Data Protection Act of Schleswig-Holstein of 9 February 2000 introduced the possibility for the Land's Data Protection Authority, the *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein* (ULD), to issue certification.

At the federal level, Section 9a of the German Federal Data Protection Act, adopted in 2001, provides that, "*in order to improve data protection and data security, suppliers of data processing systems and programs and bodies conducting data processing may have their data protection strategies and their technical facilities examined and evaluated by independent and approved appraisers, and may publish the result of the audit. The detailed requirements pertaining to examination and evaluation, the procedure and selection and approval of the appraisers shall be stipulated in a separate act.*" In practice, this particular Act was never actually implemented. Nowadays, 41 certification schemes exist in Germany. Only two seals are issued by supervisory authorities; others are issued by private entities and aim to implement the legal framework and beyond (see Chapter 6).

(continued on page 78)

Organisation	*Name of seal*	*Field*	*Type of organisation*	*Website*
Adel	ADEL (*Algorithm Data Ethic Label*)	Services / Algorithms	Private	www.adel-label.com
Cloud Confidence	Certification Cloud Confidence	Services / Cloud Services	Association	www.cloudconfidence.eu
CNIL (French Data Protection Authority)	CNIL Training Privacy Seal	Services / Training programmes	Public, issued by the Data Protection Authority	www.cnil.fr
	CNIL Processing Audit Privacy Seal	Services / Audits		
	CNIL Digital Safe Box Privacy Seal	Goods / Digital safe boxes		
	CNIL Data Protection Governance Privacy Seal	Procedures		
FEVAD (Federation of E-commerce and Distance Selling)	*Marque de confiance* FEVAD	Services / E-Commerce	Association	www.fevad.com
FNTC (*Fédération des Tiers de Confiance du numérique*)	Label E-Vote	Services / E-Vote	Association	www.fntc-numerique.com
France IT	Label Cloud	Services / Cloud Services	Association	www.label-cloud.com

Table 3. *Seals issued by French organisations*

Organisation	*Name of seal*
ADCERT Privacy Audit GmbH	ADCERT-geprüfter Datenschutz
Althammer & Kill GmbH & Co	Geprüfter Datenschutz
	Zertifizierter Datenschutz
a.s.k. Datenschutz	a.s.k. compagnysecure
	a.s.k. websecure
BNT GmbH	Geprüfter Datenschutz
Check 11 - GDD-Fachgruppe Externe Daten-schutzbeauftragte	Datenschutzzertifikat Check11
Conformity Trust GmbH	Trust in Privacy
Datenschutz cert GmbH	Zertifikat für Auftragsdatenverarbeitung
	Zertifikat für das Datenschutz-Management - Priventum
	Gütesiegel IPS (internet privacy standards)
Deutscher Dialogmarketing Verband e. V.	QuLS-Siegel Listbroker QuLS-Siegel Datenverarbeitung QuLS-Siegel Lettershop, QuLS-Siegel Adressverlag QuLS-Siegel Fulfillment
DQS Deutsche Gesellschaft zur Zertifizierung von Management-systemen GmbH	DQS-Gütesiegel Datenschutz Plus
	DQS-Gütesiegel Datenschutz
DSZ Datenschutz Zertifizierungs-gesellschaft mbH	Datenschutzsiegel

Table 4. *Seals issued by German organisations*

Field	*Type of organisation*	*Website*
Procedures, products and services	Private	www.adcert.eu
Procedures, products and services	Private	www.althammer-kill.de
Procedures, products and services	Private	www.bdsg-externer-datenschutzbeauftragter.de
Services / Websites		
Procedures, products and services	Private	www.bntgmbh.de
Individuals / Experts Data protection	Association	externer-datenschutz.de
Procedures, products and services	Private	www.conformitytrust.de
Procedures, products and services	Private	www.datenschutz-cert.de
Procedures		
Services / Online services		
Procedures, products and services	Private	www.ddv.de
Procedures	Private	www.dqs.de
Procedures, products and services	Private	www.dsz-audit.de

(Source: https://www.stiftungdatenschutz.org/zertifizierung/, February 2017)

Organisation	*Name of seal*	
ePrivacy GmbH	ePrivacySeal	
	ePrivacyApp	
editco GbR	IT-Security- und Datenschutz-Audit	
EuroPriSe GmbH	EuroPriSe (European Privacy Seal)	
Datenschutz Mecklenburg-Vorpommern	Privacy Seal Gütesiegel Datenschutz Mecklenburg-Vorpommern	
GDD (Gesellschaft für Datenschutz und Datensicherheit)	Zertifizierung der Datenschutzqualifikation	
GDI Gesellschaft für Datenschutz und Informationssicherheit mbH	GDI - zertifizierter Datenschutz	
GenoTec GmbH	Datenschutz-CheckUp mit Zertifikat	Proced
Greeneagle certification GmBH	Datenschutzkonform	
	Geprüfte Auftragsdaten- verarbeitung	
IITR (Institut für IT-Recht) GmbH	Datenschutz-Status Qualifizierter Datenschutz	
INOIS (Institut für organisatorische Informationssysteme)	Zertifizierter Datenschutz	
Interev GmbH	Geprüfter Datenschutz durch Interev	

Field	*Type of organisation*	*Website*
Procedures, products and services	Private	www.eprivacy.eu
Services / Mobile phone applications		
Procedures, products and services		
Products, services / websites	Public, issued by the Data Protection Authority; Private since 2014	www.european-privacy-seal.eu
Procedures and products	Public, issued by the Data Protection Authority; Works with EuroPriSe	
Individuals / Data protection experts	Association	www.gdd.de
Procedures, products and services	Private	www.gdi-mbh.eu
ures, products, services and individuals	Private	www.geno-tec.de
Procedures, products and services	Private	www.greeneagle-certification.de
Procedures, products and services	Private	www.iitr.de/zertifizierung.html
Procedures, products and services	Private	www.inois.de/leistungsspektrum/zertifizierung
Procedures, products and services	Private	www.interev.de

Organisation	*Name of seal*	
Legitimis GmbH	Statement of Compliance	
MediaTest digital GmbH	Trusted App	
Privacy Stiftung	ADV Compliance Checked	Proced
SCHUFA Holding AG	SCHUFA-DatenschutzSiegel	Procedu
Tacticx GmbH	Geprüfter Datenschutz	Proced
Tekit Consult Bonn GmbH (TÜV Saarland Gruppe)	TÜV Geprüfter Datenschutz	Proced
Trusted Shops GmbH	Trusted Shops	
TÜV Informationstechnik GmbH	TÜVIT-Zertifikat Trusted Site Privacy	Procedu
TUV Rheinland	Data Privacy Certification for Companies	
TÜV SÜD sec-IT GmbH	S@fer-shopping	
TÜV SÜD sec-IT GmbH	Zertifizierte Auftrags-datenverarbeitung	
Verband für Berater, Sachverständige und Gutachter im Gesundheits- und Sozialwesen e.V.	VBSG-Datenschutzsiegel	
ULD (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein)	Datenschutz-Gütesiegel	Proced

Field	*Type of organisation*	*Website*
Procedures	Private	www.legitimis.de
Services / Mobile phone applications	Private	www.mediatest-digital.com
ures, products and services	Private	www.privacy-stiftung.de
ures, products, services and individuals	Private	www.schufa.de
ures, products and services	Private	www.tacticx.de
ures, products and services	Private	www.tekit.de/zertifizierung/
Procedures / E-Commerce	Private	www.trustedshops.com
res, products and services / Websites	Private	www.tuvit.de
Procedures	Private	www.tuv.com
Procedures / E-Commerce	Private	www.safer-shopping.de www.tuev-sued.de/sec-it
Procedures	Private	www.tuev-sued.de www.tuev-sued.de/sec-it
Procedures	Association	www.vbsg.org
ures, products and services	Public, issued by the Data Protection Authority	www.datenschutzzentrum.de

Country of origin	Organisation	Name of seal
Austria	Handelsverband	TrustMark Austria
Belgium	BeCommerce	Label Becommerce
Denmark	E-handelsfonden	E-maerket
Italy	Bureau Veritas (Italie)	Certificazione del Personale Data Protection Officer
Italy	KHC (Know How Certification)	Certificazione data protection officer e privacy consultant
Italy	TÜV Italia/TÜV SUD GROUP	Certificazione di privacy officer e consulente della privacy
Luxembourg	EuroCloud Europe a.s.b.l.	EuroCloud Self Assessment EuroCloud Star Audit
Netherlands	Alliander NV	Data Privacy and Security certification
Netherlands	Thuiswinkel	Thuiswinkel Waarborg
Netherlands	Veiligheidsbranche	Keurmerk Particulier Onderzoekbureau
Spain	APEP (Asociación Profesional Española de Privacidad)	APEP-CertifiedPrivacy
Spain	Confianza Online	Confianza Online
Spain	ISMS Forum Spain	CDPP (Certified Data Privacy Professional)
Spain	Seriedad Online	Seriedad Online
Switzerland	APPD (Association des Professionnels de la Protection des Données)	CAPD (Certificat d'Aptitude à la Protection des Données)
Switzerland		CIPD (Certificat d'Implémentation de la Protection des Données)
Switzerland	SQS (Association Suisse pour Systèmes de Qualité et de Management)	Good Priv@cy
Switzerland		SQS-OCPD (OCPD:2014; avant OCPD:2008)
United Kingdom	Comodo CA Limited	Comodo Secure
United Kingdom	The Market Research Society	Fair Data

Table 5. Seals issued by organisations located in other European countries

Field	*Type of organisation*	*Website*
Services / E-Commerce	Association	www.handelsverband.at
Services / E-Commerce	Association	www.becommerce.be
Services / E-Commerce	Association	www.emaerket.dk www.emaerket.dk/english
Individuals	Private	www.bureauveritas.it
Individuals/ Data Protection experts	Private	www.khc.it
Individuals/ Data Protection experts	Private	www.tuv.it
Services / Cloud Services	Association	www.eurocloud-staraudit.eu
Products / Smart meters	Private	www.alliander.com
Services / E-Commerce	Association	www.thuiswinkel.org
Procedures / Investigation by private detective agencies	Association	www.veiligheidsbranche.nl
Individuals / Experts Data protection	Association	www.apep.es
Services / E-Commerce	Association	www.confianzaonline.es
Individuals / Data protection experts	Association	www.ismsforum.es
Services / Websites	Private	www.seriedadonline.es
Individuals / Data Protection experts	Association	www.appd.ch
Individuals / Data Protection experts	Association	www.appd.ch
Procedures and products	Association	www.sqs.ch
Procedures and products	Association	www.sqs.ch
Services / Websites	Private	www.comodo.com
Procedures / Market research	Association	www.fairdata.org.uk

Country of origin	Organisation	Name of seal
USA / Canada	AICPA (American Institute of Certified Public Accountants) et CICA (Canadian Institute of Chartered Accountants)	WebTrust
Canada	Deloitte et Ryerson University	Privacy by design Certification
USA	Better Business Bureau	BBB Accredited Business Seal or the Web
USA	BuySAFE Inc.	Buysafe Guaranteed Shopping
USA	CSA (Cloud Security Alliance)	CSA STAR (Security, Trust and Assurance Registry)
USA	ESRB (Entertainment Software Rating Board)	ESRB Privacy Certified
		ESRB Privacy Certified for Kids
		ESRB Privacy Certified for Mobile
USA	Gigya, Inc.	Gigya's Social Privacy Certification
USA	Google	Trusted Store
USA	IAPP (International Association of Privacy Professionnals)	Certified Information Privacy Professional (CIPP)
		Certified Information Privacy Manage (CIPM)
		Certified Information Privacy Technologist (CIPT)
USA	McaFee Secure	McaFee Secure
USA	PRIVO (Privacy Vaults Online, Inc.)	Privo Privacy Certified
		PRIVO's Safe Harbor Privacy Assurance Program Seal
USA	TRUSTArc	TRUSTe Certification APEC
		TRUSTe Certification Enterprise Privacy certification
		TRUSTe Certification TRUSTed Dat
		TRUSTe Certification TRUSTed Downloads
		TRUSTe Certification Children's Priva
Japan	JIPDEC (Japan Institute for Promotion Of Digital Economy and Community)	PrivacyMark System

Table 6. Seals issued by organisations located outside of Europe

	Field	Website
	Services / Audits	www.webtrust.org
	Procedures and products	www2.deloitte.com/ca/en/pages/risk/articles/Privacybydesign.html
	Services / Websites	www.bbb.org
	Services / E-commerce	www.buysafe.com
	Services / Cloud Services	www.cloudsecurityalliance.org cloudsecurityalliance.org/star/
	Services / Websites	www.esrb.org et www.esrb.org/privacy.asp
	Services / Mobile phone applications, websites and online videogames for children	www.esrb.org
	Services / Mobile phone applications	
	Services / Websites and mobile phone applications	www.gigya.com
	Services / E-commerce	www.google.com/trustedstores/
er	Individuals/ Data Protection Experts	www.iapp.org/certify/cipp
		www.iapp.org/certify/cipm
		www.iapp.org/certify/cipt/
	Services / Websites	www.mcafeesecure.com/
	Services/ Websites, games and applications for children	www.privo.com
	Procedures and products	
	Procedures	www.trustarc.com/privacy-certification-standards/
	Procedures	
a	Services / Online advertising	
	Services / Software	
cy	Services / Children under 13	
	Procedures	www.privacymark.org

(most popular organisations — non-comprehensive)

Organisme	*Nom du label*	*Objet*	*Type d'organisation*	*Site web*
EMOTA (European Multichanel and Online Trade Association)	Label de confiance de l'EMOTA	Services / E-Commerce	Association	europeantrustmark.eu/fr
Ecommerce Europe	Ecommerce Europe Trustmark	Services / E-Commerce	Association	www.ecommerce-europe.eu
EDAA (European Interactive Digital Advertising Alliance)	Trust Seal	Services / Online advertising	Association	www.edaa.eu
	OBA Certification (Online Behavioural Advertising)	Service / Behavioural advertising		
European Schoolnet	eSafety Label.eu	Services / Schools	Association	www.esafetylabel.eu

Table 7. Europe-wide seals

Outside the European Union (see Table 6, page 76), the supply of labels, marks and seals is increasingly developing in the United States. The most popular ones include TRUSTe, now called TrustArc, that provides solutions related to the principles defined by the Asia-Pacific Economic Cooperation (APEC), online advertising and protecting children below 13 years old; the Better Business Bureau (BBB), that engages with websites of companies located in the USA and Canada that comply with the BBB Code of Business Practices; the Entertainment Software Rating Board (ESRB) with its Privacy Online Seal; and WebTrust.

Some, such as TrustArc and PRIVO, provide their customers with programmes aiming to implement GDPR provisions.

Seals are issued in various fields and sectors

There are very few general seals, applicable to all sectors, on the certification market. They rather specifically focus on:

- ***products***, e.g. the Digital Safe Box Seal (*Label « Coffre-fort numérique »*) issued by the CNIL in France;

- ***services***, including mobile phone applications (e.g. ePrivacyApp by ePrivacy GmbH, Germany) and cloud computing (e.g. CSA STAR by Cloud Security Alliance, United States);

- ***processes***, e.g. Good Priv@cy, issued by the Swiss Association for Quality and Management Systems (SQS) and *Datenschutz-CheckUp mit Zertifikat*, issued by German company GenoTec GmbH;

- ***training***, on French and European texts for instance, e.g. the CNIL's Formation Seal, for:

  - data protection experts: in Spain, with the Certified Data Privacy Professional (CDPP) offered by the ISMS Forum Spain organisation; in Italy, with the Certificazione del personale-Privacy offered by the Know How Certification (KHC) organisation; and in the United States, with the Certified Information Privacy Professional (CIPP) offered by the International Association of Privacy Professionals (IAPP);

  - and, more specifically, professionals such as private detectives, e.g. the *Veiligheidsbranche's Keurmerk Particulier Onderzoekbureau* seal in the Netherlands;

- ***auditing***, with a specific CNIL seal (see Chapter 6).

Seals are issued in various fields, such as:

- ***e-commerce***: Danish mark E-maerket; BeCommerce in Belgium; Trusted Shops in Germany; and Ecommerce Europe's European Trustmark:
- ***online advertising***: German company PrivacyGmbH's OBA Certification;
- ***cloud computing***: the Cloud Security Alliance's CSA STAR in the US; the "Cloud" Seal issued by France IT;
- ***polls***: the Market Research Society's Fair Data in the UK;
- ***websites*** and online games accessible to children: Privo's Privo Privacy Certified in the USA;
- ***social networks***: Gigya's SocialPrivacy Certification in the US;
- ***education***: the European Schoolnet's eSafety Label, issued at the European level.

Different types of entities can provide seals

The seals indexed in this handbook are delivered by entities of various nature. In Europe, most of them are ***private organisations*** (56%), yet seals are also created by ***professional associations*** (34,66%) for determined fields.

► For instance, French association Cloud Confidence issues a seal for cloud computing. Association members therefore include cloud providers, service providers, experts, as well as users

The specificity of seals issued by an association is that applicants usually need to be members of the association to get certified. Besides, it is generally true that e-commerce certification is granted by professional associations including both e-sellers and service providers.

► Such is the case with Spanish seal Confianza Online and Belgian seal BeCommerce.

Certification can also be issued by ***public organisations*** (9,33%). More specifically, the seals we listed are issued by national data protection authorities, such as the French CNIL and German Länder Schleswig-Holstein and Mecklenburg-Vorpommern's authorities.

Certification is issued either by a public or a private entity, yet may follow a ***combined scheme***, depending on the nature and extent of the involvement of public authorities. Such schemes can be:

- directly managed by public authorities, e.g. seals issued by the CNIL, or have legal value;
- so-called self-regulation schemes, which authorities support without directly taking action (e.g. private seals TÜV IT and TÜV Rheinland, SQS, DEKRA, MRS/Fair Data, Trusted Shops, and OBA);
- so-called co-regulating schemes, where public authorities, as stakeholders, draw up requirements and/or take part in operational and financial management, e.g. EuroPriSe.

Switzerland's semi-public certification scheme is representative. The protection authority, i.e. the Federal Data Protection and Information Commissioner (FDPIC), takes part in the issuance, evaluation and withdrawal procedures for certification organisations. These bodies certify data processing goods and procedures in application of the Swiss Ordinance on Data Protection Certification (DPCO) adopted by the Federal Council.[2] For instance, the Swiss Association for Quality and Management Systems (SQS) is accredited to issue certification OCPD:2014. It also awards the "Good Priv@cy" seal.

5.2. …with similar certification schemes

Certification schemes are all defined by ***criteria, an assessment procedure, a logo, an ex post investigation procedure, and a conflict resolution procedure***. They aim to issue a certificate of compliance. Researcher Eric Lachaud explains that such schemes are not restricted to data protection.[3] He states that "*data protection certification is just another form of certification,*" with similar components and procedures.

2 Based on Article 11, paragraph 2 of Switzerland's Federal Act on Data Protection of 19 June 1992 (Status as of 1 January 2014) (CH301).

3 Lachaud, E. (2017). The General Data Protection Regulation and the rise of certification as a regulatory instrument. Computer Law & Security Review.

Criteria

In French, the CNIL uses the term "*référentiel*" (benchmark in English), whereas the notion of criteria is widely used in English.

A benchmark is defined in Article L 433-3 of the French Consumer Code as "*a technical document defining the characteristics that a product or a service, or a combination of products and services, should display, and the methods used to monitor compliance with these characteristics. The certification body is responsible for drawing up certification criteria, and collects the viewpoints of the parties concerned.*" It therefore usually sets characteristics, which can also be called criteria, requirements, specifications or standards. These binding elements define the activities to be certified, the criteria that should be complied with, and the threshold to be met for each criterion. They sometimes specify the range of values examiners may accept.

Data protection criteria rely on various sources — legal or not. Their contents may vary from a comprehensive framework to a concise set of requirements.

First of all, specifications are based on ***legal obligations***, which include Directive 95/46/EC on Data Protection and the GDPR, as well as national laws. Seals do not all necessarily rely on the whole set of data protection principles defined in these texts, but always refer to the main principles, namely lawfulness, proportionality, purpose limitation, and transparency.

Seals issued by Datenschutz cert GmbH are built on the German Federal Data Protection Act; those issued by the French Data Protection Authority on the French Data Protection Act (*loi Informatique et Libertés*); and both will now take into account the new provisions of GDPR.

► Displaying a seal to guarantee compliance with regulations may raise questions, since regulations are by definition binding: failure to comply with them may result in sanctions. In this respect, "*presenting rights given to consumers*

in law as a distinctive feature of the trader's offer" may be considered an unfair commercial practice.[4]

Requirements can also be based on ***recommendations by the supervisory authority***.[5]

- The CNIL certified that the French "E-voting" seal, issued to e-voting providers by the French Trusted Third Parties Federation (*Fédération Nationale des Tiers de Confiance* — FNTC), complies with the French Data Protection Act, in a deliberation dated March 17, 2016.[6]

- In Switzerland, the GoodPriv@cy and OCPD:2014 certifications, issued by the Swiss Association for Quality and Management Systems (SQS), use the Commissioner's Guidelines on the minimum requirements for a data protection management system as their benchmark.[7]

Criteria can also refer to international standards, especially those drawn up by the International Organization for Standardization (ISO). The ISO defines a standard as a "*document, established by consensus and approved by a recognised body, that provides, for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context.*"[8] Compliance with it is voluntary.

---

4 Annex 1 point 10 to Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council, EUOJ, L 149, 11.6.2005, p. 22.

5 CNIL Deliberation of 21 October 2010 relating to the security of electronic voting systems (*Délibération n° 2010-371 du 21 oct. 2010 portant adoption d'une recommandation relative à la sécurité des systèmes de vote électronique, JORF, 24 novembre 2010*).

6 CNIL Deliberation of 17 March 2016 relating to the French Trusted Third Parties Federation's "E-voting" seal project (*Délibération n° 2016-071 du 17 mars 2016 portant avis sur un projet de label « E-vote » présenté par la Fédération des tiers de confiance, JORF, 28 avril 2016*).

7 Federal Data Protection and Information Commissioner (FDPIC): Guidelines on the minimum requirements for a data protection management system (DPMS) of March 19, 2014, https://www.admin.ch/opc/fr/federal-gazette/2014/3015.pdf (FR version, also available in GE and IT)

8 ISO/IEC Directives, Part 2 — Principles and rules for the structure and drafting of ISO and IEC documents, 2016-04-30.

Some data protection seals may also be based on requirements established on the basis of a certain interpretation of standards:[9]

- ISO 27001 on information security management systems (ISMS),[10] e.g. the aforementioned Swiss SQS-OPC seal, France IT's "Cloud" seal for security and German audit company DSZ *Datenschutz Zertifizierungs GmbH's Datenschutzsiegel* seal;
- ISO 17024 on the consistent and reliable operation of certification bodies operating certification schemes for persons,[11] e.g. the APEP-CertifiedPrivacy in Spain and the *Certificazione del Personale Data Protection* issued by Bureau Veritas in Italy;
- ISO 19011 for auditing management systems,[12] e.g. the French CNIL "Auditing" seal and German companies Conformity Trust GmbH's Trust in Privacy and SCHUFA Holding AG's SCHUFA *Datenschutz Siegel*;
- ISO 29190, that provides organisations with high-level guidance about how to assess their capability to manage privacy-related processes,[13] e.g. the CNIL's Data Protection Governance seal;
- ISO 29990 on learning services,[14] e.g. the CNIL's Training seal;
- ISO 27018 on a code of practice for protection of Personally Identifiable Information (PII) in public clouds acting as PII processors,[15] e.g. the EuroCloud Star Audit certification.

Finally, criteria may rely on ***self-regulation*** mechanisms. These tools may be developed in various ways; and are usually limited in their scope to members of a group. In the field of personal data, groups are mainly professional associations that gather stakeholders from the business and online advertising fields.

---

9 To familiarise with the range of data protection standards, see *AFNOR Normalisation, Guide Protection des données personnelles : l'apport des normes volontaires* (January 2017): http://normalisation.afnor.org/wp-content/uploads/2017/02/AFNOR_Guide_Protection_des_donnees_perso_HD.pdf (FR).

10 ISO/IEC 27001:2013: Information technology — Security techniques — Information security management systems — Requirements.

11 ISO/IEC 17024 :2012: Conformity assessment — General requirements for bodies operating certification of persons.

12 ISO/IEC 19011:2011: Guidelines for auditing management systems.

13 ISO/IEC 29190:2015: Privacy capability assessment model.

14 ISO/IEC 29990:2010: Learning services for non-formal education and training — Basic requirements for service providers.

15 ISO/IEC 27018:2014: Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.

► These criteria include Spanish trust mark Confianza Online's Ethical Code,[16] BeCommerce's code of conduct for distance selling in Belgium,[17] and FEVAD's Code of Conduct for e-commerce and distance selling in France.[18]

FEVAD's Code of Conduct

The Code specifies that "*member companies commit to complying with any law and regulation on Information Technology, Files and Freedom, on Privacy and on Data Protection*" as well as with "*the code of conduct implemented by direct and digital marketing professionals.*"[19] To this end, it mentions certain legal obligations and requires all FEVAD members to comply with the French mailing opt-out list (*Liste Robinson — Stop Publicité*).

Such tool is set up by professional associations, but also by companies.

► The Market Research Society (MRS)'s "ethical" Fair Data mark certifies ten fundamental principles that supplement the British Data Protection Act and ISO standards.[20]

Evaluation process

The evaluation process aims to assess how consistent the practices of the applying entity are with the criteria. Evaluations carried out by private bodies usually lead to a service contract that binds the certification organisation and the applicant. The implementation of such contract remains uncertain, however.

Assessing data protection policies is usually carried out either through a self-assessment or an audit.

16 https://www.confianzaonline.es/documentos/Ethical_Code.pdf

17 https://www.becommerce.be/files/Code_de_conduite_du_Label_de_Qualite_BeCommerce.pdf (FR)

18 http://www.fevad.com/wp-content/uploads/2016/09/FEVAD_Codepro_Vsept2015.pdf

19 https://www.fevad.com/le-code-professionnel-de-la-fevad-se-met-de-nouveau-a-jour/ (FR)

20 http://www.fairdata.org.uk/10-principles/

Self-assessment means applying companies are required to share their data protection procedure, by answering questions, for instance; ***organisations declare what they do***. They will be granted certification if their declarations are consistent with the required criteria. This process is questionable, since checks are not always carried out (see "The misleading effect", page 125).

- American certification organisations often use this kind of "flexible" trust mark, e.g. the TRUSTe Privacy Seal (now issued by TrustArc) and BBBOnline. The European Interactive Digital Advertising Alliance (EDAA) also offers self-certification to companies that are members of the Online Behavioural Advertising (OBA) Self-Regulation Programme.[21]

- Agreements between the European Union and the United States, such as Safe Harbour — declared invalid by the European Court of Justice — and Privacy Shield, also rely on self-assessment, which has led to thorough debating and questioning among EU Member States.[22]

On the other hand, ***audits*** seek evidence. ***Organisations have to prove what they do*** by providing supporting documentation or granting access to their information system.[23] They are different from checks by nature.

Offsite auditing means applicants are required to provide documents supporting their declarations. For CNIL and EuroPriSe seals, an auditor checks consistency by comparing these documents to the criteria. To this end, they refer to the audit guidelines that detail the criteria and provide a method for objectively evaluating them. Evaluations can be strict, yet sometimes accept a certain range of deviation, which must be specified and provided for.

Finally, ***onsite auditing*** may be carried out by an evaluator to check the conformity of

21 The form can be found at: https://www.dropbox.com/s/lqkvhl31vcab2si/Self-certification%20form.pdf?dl=0. On Privacy Shield, see Letter n°5 by the Chair on Values and Policies of Personal Information, December 2016: "*Privacy Shield : un bouclier à peine brandi déjà ébréché ?*" https://cvpip.wp.imt.fr/2016/12/05/privacy-shield-un-bouclier-a-peine-brandi-deja-ebreche/ (FR)

22 See https://www.privacyshield.gov/article?id=Self-Certification-Information

23 Standard NF ISO 19011 defines an audit as "a systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled."

organisations and management systems, in addition to the examination of supporting documents in the light of the criteria. Such is the case for the GoodPriv@cy and DPCO labels, issued by the Swiss Association for Quality and Management Systems (SQS).

Most commonly, the data protection evaluation procedure is carried out internally by the certifying organisation, like the CNIL.[24] However, it can use external experts; EuroPriSe and BeCommerce have chosen Bureau Veritas as their external auditor, for instance. The external auditor can be a private organisation specialised in certification or an expert. They usually need to be accredited, in order to have more credibility. The French Trusted Third Parties Federation (FNTC) accredits external auditors who are not chosen by the applicant but randomly appointed, thus ensuring independence. In Switzerland, Swiss or foreign organisations that carry out certification as intended by Article 11 of the Data Protection Act are accredited by the Swiss Accreditation Service, which is linked to the Federal Data Protection and Information Commissioner.

Certificate of compliance

Once the data protection evaluation is carried out, if the entity meets the criteria requirements, it is declared compliant by the certifier. The certifier and the auditor can be the same body, like the CNIL. If they are not, the certifier goes through the evaluation results, decides on the conformity of the processing procedures, products and services under analysis, and issues the certificate of compliance.

Approval materialises as a certificate of compliance, which is delivered for a period of time that goes from one to five years, either by the auditor or the certification organisation. Private organisations usually charge for the certificates they issue.

Legally, certificates of compliance are usually conformity marks, i.e. trademarks. They are of two kinds: collective marks and certification marks. Eight EU Member States (Belgium, France, Germany, Luxembourg, Netherlands, Portugal, Spain, United Kingdom) have implemented a specific legal framework on certification marks.

24 Fair Data, Trusted Shops, Confianza Online, TÜV Rheinland, DEKRA Certification, TÜV IT, SQS, etc.

Transparency

To build trust with clients, certification requires transparency and therefore publicity. In practical terms, certified companies can be granted a logo representing the seal, which may also feature the seal number and its expiring date. Certified companies may display the logo on their website and communication materials as a way of standing out from competitors. To prevent frauds — there are cases of fraudulent use of logos[25] — the logo can be digitally signed by the certification organisation's website, allowing the certified company to insert a hyperlink to it on their own website.[26] The logo can also be hosted on a server controlled by the certifying organisation.[27]

Logos are physical markers meant for the public and clients of the certified company, as they show it complies with the criteria and is therefore trustworthy. Yet such trust marks have to be known and easily recognisable, which implies implementing a communications strategy — this is actually hardly ever done. Media coverage, however, is a useful tool for a seal to be efficient, as the case of the French "*Label Rouge*" shows — it has become a renowned sign of quality assurance in France.

Logos are not the only visible sign of certification. Sometimes, the public and clients can have access to the underlying documents that led to certification, such as the auditor's report and the certification organisation's conformity conclusions. Yet, few, apart from EuroPriSe and EuroCloud Star Audit, have agreed to publish these reports. Some organisations do however publicly upload a register of companies[28] they have certified, together with their certificate of compliance.[29]

---

25 In the United States, TRUSTe sued websites American-Politics.com and SurfAssured.com for displaying the trust mark without being certified. Standards in Electronic Transactions v Underwriters Digital Research Inc., US DC (Columbia), Civil Action No. 00–02574(CK).

26 E.g. PrivacyMark (online); Danish E-maerket; MRS Fair Data.

27 E.g. the Ecommerce Europe Trustmark, that is linked to a certificate, just like the participation national associations' national trust marks. In order for the certificate to be used, the logo has to be linked to the following address: https://ecommercetrustmark.eu/name-of-your-national-association.

28 E.g. Confianza online; Seriedad online; Good Priv@cy.

29 E.g. Danish E-maerket; ePrivacySeal.

Investigations, remedies and sanctions

Informing the public also implies implementing conflict-resolution mechanisms, in the interest of all parties, in the case a dispute should occur between the certified company and the individual whose data is used. However, it appears that most existing seals do not communicate on such mechanisms (see Chapter 7).

How to cite this chapter: Levallois-Barth C., Chauvet D. “A French, European and international overview of personal data protection certification”, *in Signs of trust – The impact of seals on personal data management*, Paris, Handbook 2 Chair Values and Policies of Personal Information, Coordinated by Claire Levallois-Barth, January, 2018, chapter 5, pages 63–89.

http://www.personal-information.org/

Chapter 6.

Certifying for compliance: implementing the policy framework and beyond

Claire Levallois-Barth
Delphine Chauvet

6

Out of all seals in keeping with the data protection legislation, two case studies hold interesting lessons: the seals delivered by the French Data Protection Authority, called CNIL, in France (6.1) and those by EuroPriSe in Germany (6.2).

► The EuroPriSe seal was developed as part of a 2007 research project funded by the European Commission, under the leadership of the Data Protection Authority of Schleswig-Holstein (*Unabhängiges Landeszentrum fuer Datenschutz* — ULD). It is now issued by a private company in partnership with supervisory authorities.

It should be pointed out that these compliance certifications are equally demanding. However, their material and territorial scopes of application do not really intersect. Besides, while one could imagine that involving data protection authorities would be a sign of trust and durability for the general public and companies, these seals are still limited to "niche" cases and to relatively few entities, and are not well-known by the general public. This is mainly because obtaining them is costly, sometimes very costly, and their criteria are too strict, according to some stakeholders. Their return on investment is far from being an incentive. (6.3)

Certifying for compliance: implementing the policy framework and beyond

6.1. The CNIL's Privacy Seals

In practice, certification is a complex issue both for lawmakers and data protection authorities. In this respect, the CNIL's certification powers were defined step by step. The process started in 2004 and is far from being completed, since the CNIL now has to adapt its criteria to the new GDPR requirements (see Chapter 8).

Four different seals

As of July 31, 2017, the CNIL issues four types of seals.

In 2004, a law allowed the CNIL, "*when requested by professional organisations or institutions of which the members are mainly data controllers" to deliver "a privacy seal to products or procedures.*"[1] However, it only issued its first seal in 2011.

1 Art. 11, 3-c) of Act No 2004-801 of 6 August 2004 on Protection of Individuals with regard to the Processing of Personal Data amending Act No 78-17 of 6 January 1978 on Data Processing, Files and Individual Liberties, JORF, 7 August 2004.

Exercising certification power implied passing an implementing decree, which was in fact never published, since the French Department of Civil Affairs and the Seal (*Direction des Affaires Civiles et du Sceau* — DACS), had trouble addressing "*the competitive issue of differentiation by quality.*"[2] The situation changed in 2009 when the law authorised the CNIL's rules of procedure to specify "*the implementing modalities of the certification procedure,*"[3] making a decree useless.

Around the same time, the CNIL was allowed to go through independent and qualified third-party auditors "*when justified by product or procedure complexity;*" it being specified that "*the cost of such an audit is borne by the company applying for the seal.*"[4] It took the CNIL two years to amend its rules of procedure.[5]

In 2014, the Law on consumer rights (*Loi Hamon*) enabled the CNIL to "*determine, on its own initiative, if a product or procedure is capable of benefiting from a privacy seal*"[6] (see frame below, Article 11, 3° (c) of the French Data Protection Act).

Finally, since October 7, 2016, the French DPA has been able to certify data anonymisation procedures and approve related criteria and general methods.[7] This was allowed by the French Act for a Digital Republic (*Loi Lemaire*), which includes principles such as Open Data and provides that using anonymisation procedures should reconcile the general interest (making use of data and informing citizens) with the interest of individuals (protecting their personal data). It is still unknown when and how the CNIL will take that power (see frame below, Article 11, 2° (g) of the French Data Protection Act).

---

2 Interview with Yann Padova, CNIL Secretary General from 2006 to 2011.

3 Art. 105 of the French Act of 12 May 2009 simplifying and clarifying the law and alleviating procedures (*Art. 105 de loi n° 2009-526 du 12 mai 2009 de simplification et de clarification du droit et d'allègement des procédures*, JORF, 13 May 2009).

4 Art. 105 of the *Act n°2009-526*, aforementioned.

5 CNIL Deliberation of 8 September 2011 amending Article 69 of the CNIL's internal rules and policies and introducing Chapter IV bis entitled "Certification process" (D*élibération n° 2011-249 du 8 sept. 2011 portant modification de l'article 69 du règlement intérieur de la Commission nationale de l'informatique et des libertés et insérant un chapitre IV bis intitulé « Procédure de labellisation »*, JORF, 22 September 2011). See the latest version of the CNIL's Rules of procedure, *Délibération n° 2013-175 du 4 juillet 2013 portant adoption du règlement intérieur de la Commission nationale de l'informatique et des libertés.*

6 *Art. 17 of the French Act on Consumption (Art. 17 de la loi n° 2014-344 du 17 mars 2014 relative à la consommation*, JORF, 18 March 2014)

7 Act for a Digital Republic (*Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique*, JORF, 8 October 2016).

Article 11, 3° (c) of the French Data Protection Act

« It [the CNIL] shall deliver a privacy seal to products or procedures intended to protect individuals in respect of processing of personal data, once it has recognised them to be in conformity with the provisions of this Act. In the context of prior examination of privacy seals by [the CNIL], [the CNIL] can also determine, on its own initiative, if a product or procedure is capable of benefiting from a privacy seal. The president can seek the evaluation of an independent qualified person, when justified by the complexity of the product or of the procedure. The cost of such evaluation shall be borne by the company requesting the privacy seal; the Commission can withdraw the privacy seal if it finds, by any means, that the conditions that allowed for the accordance of the privacy seal are no longer fulfilled. »

Article 11, 2° (g) of the French Data Protection Act

« It [the CNIL] may certify or approve and publish criteria or general methods to certify compliance with this personal data anonymisation process, in particular in order to reuse public information disclosed online. »

In practice, it appears certification is a complex issue for supervisory authorities. In 2009, this emerging activity required the CNIL to acquire the technical means and legal resources, especially in terms of competition law, in order for it to certify products. One of the questions raised was that of "positive discrimination" towards certain products and services.[8]

A merit of the CNIL was it dared engaging in the process, faced with a lack of propositions on the business side. Indeed, unlike Germany (see Chapter 7), France did not historically rely on certification much.

For neutrality purposes and probably because of the little impact it has on the marketplace, the CNIL started tackling the least challenging issues in terms of interaction and

8 Naftalski F. and Desgens-Pasanau G., (2010). *Enjeux et perspectives du pouvoir de labellisation de la CNIL, Revue Lamy Droit de l'Immatériel*, N°63, August/September 2010, 12 pages.

consequences. Therefore, it decided to pass two sets of criteria in October 2011; one on training and another on auditing. The ***Training*** Privacy Seal is delivered to organisations that offer in-house or external data protection training programmes, including e-learning programmes. The ***Processing Audit*** Privacy Seal may be requested by service providers (consultancies, lawyers, etc.) that sell data processing audit procedures, or by organisations that implement such procedures in-house. These procedures define the steps and processes to plan, carry out and complete audits. These two seals therefore do not apply directly to the personal data processing implemented by organisations.

In January 2014, the CNIL passed its criteria on digital safe boxes, and in December 2014, those on data protection governance (*Gouvernance Informatique et Libertés*). The ***Digital Safe Box*** Privacy Seal relates to digital box services that store personal data (documents, some metadata). Such data is only made accessible to the safe box holder and any people they may have mandated. The ***Data Protection Governance*** Privacy Seal focuses on data protection procedures implemented by organisations, including regular in-house or external audits. This certification thus has a more ambitious scope.

These two seals were created at the request of professional organisations and institutions that bring together data controllers. The Data Protection Governance seal was requested by the French Association of Data Protection Officers (A*ssociation Française des Correspondants aux Données Personnelles* — AFCDP); and the Digital Safe Box Seal by the French Trusted Third Parties Federation (*Fédération des Tiers de confiance du numérique* — FNTC). In all four cases, the CNIL reckoned the seal was meant to meet a market need.

All four assessment criteria are based on legal standards, and some on CNIL recommendations or ISO standards. They were drawn up by the CNIL's Certification Committee,[9] made up of three Commissioners appointed by the CNIL Chair, then adopted after a deliberative process in its plenary session. The Governance Seal criteria were partly based on the GDPR draft regulation as well as on standards ISO/IEC 27001:2013 on Information security management systems (ISMS) and ISO/IEC 29190:2015 on Privacy Capability Assessment Models, that were both adapted to Data Protection Officers' prac-

9 The Certification Committee is responsible for offering guidance on the CNIL's certification policy, drawing up draft criteria and assessing the conformity of applicants. It convenes every three months.

tices. The Governance Seal also differs in the way it was drawn up, as its 25 criteria were established with the help of the AFCDP.

The CNIL never followed up on some requests, including those on “Cloud Computing”, “Cookies” or “Online Payment” seals. It rejected the French General Medical Council’s request for a certification for e-health mobile applications because of how complex it is to certify a mobile app relying on an operating system and its specific design choices, especially in terms of configuration.

Therefore, the four privacy seals issued by the CNIL have different scopes, but a similar issuance procedure.

Name of certification	*Field*	*Basis for criteria*	*Year of creation*	*Duration*	*Number of awarded seals*
CNIL Training Privacy Seal	Services / Training	Legal standards + ISO 29990	2011	3 years	54
CNIL Processing Audit Privacy Seal	Services / Audit	Legal standards + ISO 19011	2011		25
CNIL Digital Safe Box Privacy Seal	Services / Digital safe boxes	CNIL recommendations	2014		1
CNIL Data Protection Governance Privacy Seal	Procedures	Legal standards + ISO/IEC 27001:2013 + ISO/IEC 29190:2015 + RGPD draft	2014		13

Table 8. Privacy Seals issued by the CNIL as of October 17, 2017 [10]

10 NF Standard ISO 29990: Learning services for non-formal education and training — Basic requirements for service providers, 2010.

NF Standard ISO 19011: Guidelines for auditing management systems, 2002.

Standards ISO/IEC 27001:2013 on Information security management systems and ISO/IEC 29190:2015 on Privacy Capability Assessment Models, adapted to Data Protection Officers’ practices.

The CNIL's certification process

Although the CNIL has the right to resort to independent third parties, it has chosen to take responsibility for assessment and certification issuance, according to the following four steps:[11]

1. **Request:** Any legal person may request a seal; only a natural person may request the Training seal. Two or more entities can file a joint request. A request may be submitted by downloading the application file on the CNIL's website,[12] filling it out, and mailing it or submitting it online.

2. **Admissibility:** Once the request has been filed and the applicant has been given a registration number, the CNIL Chair has two months to decide on the admissibility of the application. The Chair is deemed to have refused the request if no response is sent to the applicant within two months. A request may be rejected if it does not fully fall in the scope of the criteria or if the file is incomplete..

3. **Investigation by the CNIL:** Once a request is deemed admissible, the CNIL Seal Section, made up of two people from the Compliance Department, investigates the application. As explained on the CNIL's website, "*the length of an investigation varies according to the initial compliance rate and the extent of communication with the [CNIL].*" In practice, investigators carry out several assessments until total compliance is reached. The length of the assessment varies depending on how complex the case is, whether additional information is needed and whether the Seal Section or the Certification Committee carry out an audit. It is usually close to seven months. The Certification Committee then decides on the conformity of the application.

4. **Issuance:** The CNIL issues seals for a period of three years, renewable, in plenary session. If a request is rejected, it is not made public; and application files, which may include audit quizzes for instance, cannot be released as provided by the

11 See a more detailed figure in Naftalski F., (2011). *Label CNIL et conformité « informatique et libertés : publication des premiers référentiels, Revue Lamy Droit de l'Immatériel*, 8 pages

12 As an example, see the CNIL Data Protection Governance Privacy Seal application form, https://www.cnil.fr/sites/default/files/atoms/files/labelsCNIL-gouvernance-demande_0.docx

French Freedom of Information Act.[13] Applicants may refer to the Council of State within a period of two months. This has so far never occurred in practice. Applicants who are granted certification are notified by mail and receive personalised logos together with their regulation for use. The CNIL's deliberation is published in the Official Journal through the *Légifrance* website as well as on the CNIL's website. The list of certified products and procedures, seal recipients and seal expiration dates, is thus made available to the public.

Organisations that have received a seal are ***required to submit an activity report*** with the CNIL after the first year of the grant, in order for it to check compliance with the criteria and ensure that the "CNIL Privacy Seal" logo is used in compliance with the regulation governing use of the collective mark. The regulation provides that "*the logo should be used in direct relation to the certified product or procedure. Affixing a logo in an unspecific and undifferentiated manner is strictly prohibited.*"[14] This prevents companies that provide one certified service from extending certification to all of their services, which may be subject to sanctions under the heading of misleading advertising or unfair competition.

Example of logo and expiration date.

13 The French Commission for Access to Administrative Documents (*Commission d'Accès aux Documents Administratifs* — CADA) told the CNIL these files came within the exception laid down by Article 66-II of the Law of 17 July 1978 with regard to the protection of commercial and industrial confidentiality, (*Loi du 17 juillet 1978 au regard de la protection du secret en matière industrielle et commerciale*).

14 See Regulation governing use of the CNIL Privacy Seal collective mark, https://www.cnil.fr/sites/default/files/atoms/files/label_CNIL-charte_dutilisation_du_logo.pdf (FR)

The CNIL may also assess compliance with the criteria at any time. The seal holder is informed in advance; there are no spot checks, as the CNIL aims to "*assist, guide, promote and encourage the behaviours of organisations who are trying to make a difference.*"[15] Up to now, a few checks have been carried out, on the Training Privacy Seal only.

When a complaint is filed by a third party, or if the CNIL thinks there might have been a breach of the criteria, the certified entity is required to share its observations within a month. If its answers are deemed unsatisfactory, a rapporteur is appointed among members of the Certification Committee. The plenary session then decides whether they should withdraw the seal — which has never happened so far.

The seal renewal procedure is not as complex: six months before the seal expires, the certified entity should inform the CNIL whether it wishes to have it renewed and indicate changes should there be any, in which case these are checked.

CNIL Privacy Seals will most likely be of interest to French organisations mainly. Yet, if they prefer to get a European seal, they can request the EuroPriSe seal, which has a partnership with the CNIL.

6.2. The European EuroPriSe Seal

The trans-European EuroPriSe seal — which stands for European Privacy Seal — allows organisations to show compliance with European laws and regulations. Its main difference with CNIL seals is that independent experts are entitled to conduct evaluations.

A seal of excellence created and supported by European Data Protection Authorities

EuroPriSe was created in 2007, an outcome of the eTEN programme, funded with 1.2 million euros by the European Commission. The project consortium, led by Germany's Schleswig-Holstein Data Protection Authority (*Unabhängiges Landeszentrum fuer*

15 Carvais, J. (2015). *Le label CNIL comme outil de conformité, in AFCDP, Correspondant Informatique et Libertés, Bien plus qu'un métier*, pp. 504.

Datenschutz — ULD), included about ten partners from eight European countries, among which data protection authorities, universities and consultancies.[16]

After two years of development, EuroPriSe published its criteria for "IT Products and Services". Under these criteria, seals are granted to entities of all sizes, SMEs as well as multinational companies such as Microsoft (2008) and SAP (2012).

On January 1st, 2014, the project was transferred to a private company, EuroPriSe GmbH, which now features a Certification Authority responsible for issuing seals, as well as an Advisory Board in charge of ensuring seal quality.

The board is made up of independent experts from protection authorities, including a representative from ULD and another from the CNIL.

Since 2014, EuroPriSe has worked as a certification authority for the privacy seal of the German federal state of Mecklenburg-Vorpommern, in consultation with the Land's Commissioner for Data Protection and Freedom of Information.[17] The seal, called *Gütesiegel Datenschutz Mecklenburg-Vorpommern* (seal of approval) relies on Article 5 of the Data Protection Act of Mecklenburg-Vorpommern and certifies compliance with the Act. The Act compels the Land's public bodies to deploy certified products and procedures in priority and give competitive advantage to certified companies.

In April 2016, EuroPriSe GmbH expanded its activity by offering certification for websites; it now covers publicly available parts of websites and focuses on the interaction between a web server and a visitor's browser.

Unlike the CNIL, EuroPriSe does not use different sets of criteria for each of its seals, but one unique criteria catalogue that specifies, if needed, whether a requirement is applicable

16 Including the data protection authorities of Madrid (Agencia de Protección de Datos de la Comunidad de Madrid — APDCM), and France (*Commission Nationale de l'Informatique et des Libertés* — CNIL), the Austrian Academy of Science, the London Metropolitan University from the UK, Borking Consultancy from the Netherlands, Ernst and Young AB from Sweden, TÜV Informationstechnik GmbH from Germany, and VaF s.r.o. from Slovakia.

17 https://www.european-privacy-seal.eu/EPS-en/News/n/7972/europrise-starts-work-as-certificationauthority-for-the-new-privacy-seal-of-the-german-federal-state-of-mecklenburg-vorpommern

to a product, a service or a website.[18] The catalogue lists relevant questions and is often updated, as shows the 109-page version published in January 2017. This version integrates the requirements of the GDPR, the ePrivacy Directive, as well as Member States' current legislations. Relying on such high-level data protection may infer influence from data protection authorities, especially ULD, which is sometimes seen as one of the strictest European authorities. This explains why EuroPriSe refers to its seal as a "*trust mark of excellence*" openly aiming to give certified companies competitive advantage.

EuroPriSe's certification process is as strict as its legal and technological criteria.

EuroPrise experts are involved in the certification process

Just like CNIL Privacy Seals, EuroPrise seals are issued following a four-step procedure. The whole process, from submission to experts to seal issuance, usually takes from eight months up to a year.

1. **Pre-evaluation:** Applicants choose a legal expert and a technical expert from EuroPriSe's public register of approved experts. They introduce them to their product, service or website and discuss assessment modalities, especially the scope of certification (Target of Evaluation — ToE). Then, they refer to the EuroPriSe certification authority, which approves the ToE during a preparatory meeting. Applicants negotiate experts' fees, before laying down an agreement with the Certification Authority.

2. **Evaluation by experts:** Both experts assess the product, service or website. They especially identify all personal data flows related to the certification scope and make sure they are legally compliant with European laws. Then, they write two joint reports: a confidential evaluation report and a short public report. They are also required to make written declarations and, for each evaluation, act with complete independence.

18 EuroPriSe Criteria for the certification of IT products and IT-based services ("GDPR ready" version — January 2017): https://www.european-privacy-seal.eu/EPS-en/Criteria

Words of a EuroPriSe expert

"We have to define our target, the scope of what we want to certify… It is a tedious, difficult task. We go through all [data] flows, identify them and make sure they are compliant with all European acts; not only the Directive and legal precedents, but the Article 29 Working Party opinions as well…"

3. **Validation by the Certification Authority:** Applicants approve both reports and share them with the Certification Authority, which carries out a re-evaluation to check whether relevant criteria were applied and whether the applicant responded to questions plausibly. In the particular case of the Mecklenburg-Vorpommern seal, the opinion of the EuroPriSe certification authority is passed on to the Commissioner for Data Protection, who then gives their approval.

4. **Issuance:** Seals are awarded for a renewable period of two years. The renewal procedure is not as strict as the certification procedure. Awarded seals are made public at https://www.european-privacy-seal.eu/EPS-en/awarded-seals, along with their validity period and the short public report (downloadable). Certified organisations also receive a certificate of compliance. Having a register of approved experts enables transparency; as does having a dispute resolution system. Complainants should follow a two-step procedure: first address the seal holder directly, and if things are not solved, fill out an online form so that EuroPriSe GmbH may carry out an investigation.[19] As far as we know, EuroPriSe has never carried out a withdrawal procedure so far.

Excellence is also demonstrated through the strict expert admission procedure, which focuses on three main criteria: qualification, reliability, and independence.[20]

19 https://www.european-privacy-seal.eu/EPS-en/Dispute-Resolution-Complaint-Form

20 https://www.european-privacy-seal.eu/EPS-en/Expert-Admission

The three requirements for EuroPriSe expert admission

Qualification: Experts attend an admission workshop and follow a mandatory three-day training in English that focuses on evaluation and auditing, at the end of which they write a joint report based on a practical case together with their legal or technical counterpart. It usually takes 15 days for an already specialised expert to be admitted.

Reliability: Experts are required to provide self-declarations on their financial background (no insolvency proceedings, for instance), criminal background (no conviction for fraud or document fraud in the last five years) as well as their liability insurance, that should cover possible damages that could occur during evaluations.

Independence: Experts cannot be the Data Protection Officer or consultant for the applying organisation.

After admission, experts receive a logo specifying their area of expertise (see above). They are subject to an annual fee of €390 (VAT excluded). If they wish to extend their admission to website certification, they are required to conduct a training evaluation and to submit a report on it once again. They are then subject to an additional €150 (VAT excluded) or, if they are not already accredited, €600 (VAT excluded). In order to extend their three-year admission, they have to conduct a EuroPriSe evaluation. If no evaluation has been conducted, they have to participate in a workshop to update their knowledge.

In spite of this, the EuroPriSe seal is not more popular than CNIL Privacy Seals, thus not helping users to make their way through the profusion of data protection products and services. Why so?

6.3. Little public awareness and limited return on investment

There are still relatively few certified entities, be it with EuroPriSe or the CNIL Privacy Seals. The reason might be that obtaining such trust marks is extremely costly, while return on investment is still limited.

Few certified entities

In June 2017, 19 entities, most of them German, had been awarded the EuroPriSe seal. Over the past ten years, including renewals, there were:[21]

- 6 seals awarded in 2008
- 6 seals awarded in 2009 (and 1 renewal)
- 3 in 2010
- 5 in 2011 (and 2 renewals)
- 3 in 2012 (and 2 renewals)
- 2 in 2013 (and 3 renewals)
- 8 in 2014 (and 3 renewals)
- 5 in 2015 (and 6 renewals)
- 3 in 2016 (and 3 renewals)
- 2 in 2017 (and 8 renewals)[22]

A EuroPriSe admitted expert explains: "*I was very disappointed with return on investment.*" This person put in time (one month minimum), expertise (significant knowledge of all decisions taken at the European level) and money to get certification and still has not conducted any evaluation. This is not the only example; by the end of June 2017, around a hundred people, located in 19 countries, were listed on the Register of Experts.[23]

The CNIL has delivered many more seals, 93 in total, among which:

- 54 Training Seals (and 21 renewals)
- 25 Process Auditing Seals (and 9 renewals)
- 1 Digital Safe Box Seal
- 13 Governance Seals

21 All data was updated in December 2017.

22 https://www.european-privacy-seal.eu/EPS-en/awarded-seals

23 https://www.european-privacy-seal.eu/EPS-en/register-of-experts

As a comparison — limited as it might be — in France:

- in the organic farming sector, 32,236 producers held the Organic Farming certification (*Agriculture Biologique* — AB) end of 2016;
- • in the agro-food industry, more than 5,000 farmers (i.e. 97,093 chicken) have the *Label Rouge*;
- • in the environment sector, 142 companies had the NF-Environnement mark in 2005.

In the United States as well, many companies hold data protection certification. The *TRUSTe Certified Privacy Seal*, now issued by *TrustArc*, has been awarded to more than 1,000 clients,[24] while the BBBonline seal has been granted to 145,700 websites. These numbers should yet be used with caution, since American requirements are not as strict as European ones — self-certification is possible under some of these schemes (see Chapter7).

Let us also consider the number of seals awarded by the ULD, the Data Protection Authority of German Land Schleswig-Holstein. Like for EuroPriSe, evaluations are carried out by admitted experts who have proven their legal and/or technical expertise. They result in a report validated by the ULD, which then issues certification.

With this certification procedure, since 2002:

- 96 seals have been awarded to products and services at the Land level (and 47 renewals);
- 84 experts have been admitted since 2002, including 38 legal experts, 24 technical experts, and 22 experts in both fields;[25]
- no seal has been awarded by the Land of Mecklenburg-Vorpommern.[26]

24 TrustArc by Numbers: https://www.trustarc.com/resources/privacy-research/trustarc-by-the-numbers/

25 Privacy Seals and Certifications, Databeskyttelsesdagen 2017, Babara Körffer, Unabhaengiges Landeszentrum fuer Datenschutz, Schleswig-Holstein Tyskland, https://databeskyttelsesdag.files.wordpress.com/2017/01/dk_privacy-seals-and-certifications_2017-2.pdf

26 https://stiftungdatenschutz.org/aufgaben/zertifizierung, February 2017.

How is it that so few entities are certified with either the EuroPriSe or the CNIL Privacy Seals?

An interviewee told us this is only the beginning of a long process and there will be more seals when the GDPR is implemented (see Chapter 8). An expert from a certification organisation emphasised that the goal is not to reach a certain number of organisations, rather to attract "*several popular and valued brands*" so as to have a multiplier effect and stimulate certification requests.

For this to happen, several requirements need to be met; including greater public knowledge on data protection certification — and we are still far from a tipping point for both the public and entities to reach broad awareness of these trust seals. Very few in France know about CNIL Privacy Seals, compared with agro-food and energy seals. People are more worried about the health risks related to the quality of the environment than personal data protection, which certainly represents a less concrete and more distant risk. In Europe, unlike in the United States, consumers' associations actually barely ever address the issue, which they consider too technical (see Chapter 7). However, it appears users/consumers are adapting their behaviours to new customs and techniques, as shows the recent survey carried out by the Chair Values and Policies of Personal Information together with Médiamétrie (see Chapter 10).

Besides, the CNIL rarely promotes its Privacy Seals and rather gives more coverage to other aspects of its work. For its part, EuroPriSe cannot afford coverage, even though many EuroPriSe admitted experts work in major consultancies and law firms, especially in Spain, the United Kingdom and Sweden. During interviews, most of them admitted they did not communicate on this enough, due to time constraints and lack of familiarity.

In the private sector, people are not more aware of either of these certification logos, and those who are do not see it as a real benefit. Seals were designed as enforcement mechanisms for data protection regulations, but they usually prove expensive to obtain.

Significant costs for little competitive advantage

EuroPriSe is completely impartial yet very costly. For instance:

- in order to certify a very specific item, such as a biometric solution, 30 days of work are needed (15 with the technical expert; 15 with the legal expert) for a minimal cost of €40,000;

- for a larger scope, experts estimate the costs at €80,000 while others say €100,000 to €200,000;

- certifying a website requires at least 20 days of work (10 with the technical expert; 10 with the legal expert).

Prices are directly linked to the certification scope, which defines the amount of time experts will need and charge for. That amount is hard to define, especially for the technical part, for which "*it all depends on how many processors and service providers are involved in hosting and in security.*"

Words of a EuroPriSe expert

"Identifying data flows takes a very long time… Especially because no one knows what is going on. What makes it worse is that information checks and requests of user consent are hardly ever done the right way. Then once you're off site, it all becomes a mess! It takes ages to check all contracts and other thingies!"

Narrowing the evaluation target could be one way of reducing costs. Yet according to the four experts we talked to, certification would thus lose its meaning and the application would be rejected by the EuroPriSe Certification Authority. Certain companies actually abandoned the project during the preparatory phase for this reason. This led EuroPriSe to expand its certification scope to websites, "*in order for seals to be more marketable, because both cheaper and more publicly recognised.*"

A second way to reduce costs without reducing the scope would be to carry out an impact assessment beforehand, thus allowing to identify risks and pick out criteria at constant scope, as put forward by an expert.

Words of a EuroPriSe expert

"There is always a marginal risk that we need to accept, with proportionality as our guiding principle – i.e. depending on the data processing we are auditing, we will need to go into the smallest details as we do with health data, or when sensitive data is collected."

CNIL Privacy Seals are free of charge. Yet one should account for the time spent, which also brings about costs. Most people we interviewed said getting a CNIL seal was time-consuming, as the steps taken even turned into an "*obstacle course*" for some of them. There again, costs mostly vary according to the scope chosen and the size of the company. Interviewees told us getting the Training seal took them "*a few weeks*" for some, "*15 man-days*" for others. The Audit seal is more time-consuming, as a company estimated they spent 143.5 days (with a five-person team); another told us it took them a year and half to "*build the seal,*" and another said they spent four to five months.

While some consider certification as a strong sign of quality and trust, other emphasise the excessive administrative burden it implies. An interviewee told us "*the biggest mistake is to require more than the existing legislation, instead of enforcing the law as it currently stands.*" The Governance seal, for instance, requires the organisation to have a Data Protection Officer (DPO). Yet DPOs are merely an option in the French Data Protection Act, and the GDPR does not always require organisations to have one. One of the people we spoke to said "*people are confusing the goal (personal data protection) with the means (having a DPO) ... What matters is, can we get the same result without a DPO?*" Another person believes the CNIL is trying to "*impart its doctrine*" and add "*details that are not required by law" yet that "the regulator would want to become common practices, which discourages all stakeholders to do more than what is strictly required by law in these public seals.*"

"*The supervisory authority wants to show what makes it specific by extending the regulation and thus micro-regulating more than companies are willing to accept.*" Such tendency to "*micro-regulate*" is especially mirrored by the 33 mandatory requirements and 44 optional requirements on add-on modules to the Training Privacy Seal as well as the 73 requirements to the Audit Privacy Seal.

Words of an expert about the CNIL Training Privacy Seal

"The details and bureaucracy they ask for are complete madness. I was told, 'You forgot to include the definition of consent from Art. 2(h) of the Directive.' Since they do documentary audits, they think they need to go through all documents in order to conduct their investigation properly."

Again, what is criticised here is the fact applicants are not given enough flexibility and room for manoeuvre. An interviewee told us: "*It's not flexible enough; and some requirements are totally irrelevant compared to needs on the ground.*" Another pointed out: "*It's only theory… Theoretically, you can implement a nice procedure and check all requirements without even having been on the field."* This is especially true about the Audit Privacy Seal, which does not take into account the size and nature of organisations (consultancies, companies, etc.). Besides, unlike EuroPriSe, this seal requires gathering legal and technical competences beforehand, which means one needs to find "*their soul mate*" before even filing the request. That is a problem for some people.

The reason only one Digital Safe Box Seal has been awarded so far (in July 2016) is that one of the 22 requirements is a problem. Indeed, supplied products do not encrypt the names of files stored in digital safes. The CNIL has justified its doctrine by saying these metadata are as sensitive as the file itself.

An expert pointed to us that this kind of "*over-bureaucratisation results from the fact CNIL Privacy Seals were meant as specifications for a quality process, the way food companies or retailers do it. This breakdown approach focuses on processes rather than substance, which makes it questionable, or even sterile, as regards training.*"

Johanna Carvais, the head of the CNIL's Seals Section in 2015, explained that "*the CNIL, rather than basing certification requirements on compliance with the law, has decided to go beyond the law and ensure that the requirements used as criteria for conformity assessments mirror, at the very least, usual CNIL recommendations and general best practices. Laws are indeed applied to all; a seal that proves compliance with the law should therefore be granted to all. Yet, the strength and use of seals lie in helping make out good from bad operators. Therefore, they cannot be granted to all operators of a same market, or else they lose credibility. They should help make out which entities are certified and*

give those a proper competitive advantage. Only then will privacy seals be considered as economic assets."[27]

Different opinions have been expressed on the extent of CNIL Privacy Seals' return on investment. Some say being certified "*didn't help them sell more.*" Others, especially law firms and consultancies, believe being certified has helped them attract more clients. They view seals positively, as a competitive asset, especially when working B2B with public organisations on public procurement. In this respect, Schleswig-Holstein's Data Protection Act provides that preference shall be given to certified products,[28] while the Swiss Federal Law provides that the controller of data files is not required to declare their files if they have acquired a data protection quality mark.[29]

Words of experts on the Training Privacy Seal

"Never has a customer told us, 'I chose you because you are certified'. I don't think it has increased the number of my clients at all. That is weird!"

Yet paradoxically, many holders of CNIL certification apply for renewal: "*I am reapplying for the Training Seal to improve my image.*"[30] EuroPriSe-admitted experts renew their admission for the same reasons.

In France, some CNIL-certified organisations that spent time acquiring a seal are considering requesting another. Since they have already taken care of the "clearing" part and know how to work with CNIL methods, they believe requesting another seal will not be as time-consuming.

27 Carvais J., (2015). *Le label CNIL comme outil de conformité, in AFCDP, Correspondant Informatique et Libertés, Bien plus qu'un métier*, pp. 500.

28 Art. 4§2 of the State Data Protection Act of the Land of Schleswig-Holstein.

29 Art. 11a, recital 5, Swiss Federal Act on Data Protection of 19 June 1992 (Status as of 1 January 2014) (CH301).

30 More specifically, nearly 100% of Training Privacy Seals and 50% of Audit Privacy Seals get renewed.

Words of an expert

"It took me 15 man-days to get the CNIL Training Seal. I think it'll take me 10 to get the Audit Seal."

Let us keep in mind that certification procedures and processes are fairly new with respect to data protection. Adapting and generalising them, both on the economic and social levels, necessarily requires time. As a lawyer mentioned, "*this is only the beginning of a long story.*"

What about organisations that do not have CNIL certification?

As it is too early to evaluate the economic benefits of these seals, the time and money invested need to be compared with the benefits that companies expect. And so far, these benefits have usually not been high enough, especially since risks of non-compliance have been relatively limited. Civil and criminal penalties are currently pretty much non-existent. The 13 sanctions the CNIL adopted in 2016 (4 financial penalties and 9 warnings, 4 of them public) clearly had little impact. Indeed, the CNIL is not an enforcement authority. Will it become one when the GDPR comes into force and the CNIL is in a position to adopt financial penalties up to 20 billion euros or up to 4% of the worldwide annual turnover?

Words of experts on the CNIL Governance Seal

"No one wanted to do it… Companies have taken a wait-and-see approach on the new French legislation. This has to do with the absence of sanctions. It's enterprise risk management." "[...] Data breaches are not punished enough; if they were, companies would probably use that tool. But they aren't, so what's the point?"

Even with higher financial penalties, companies do not view certification as a simple extension of the law. It is hard to find common ground "*between what the CNIL wants to promote through its seals and what companies want to show by being certified*", which in the case of companies goes well beyond the mere desire to emphasise their compliance.

Words of an expert

"The communication the company wishes to develop is facing a dead-end, because the only thing the company hopes for, which can bring a positive return on investment, is a seal that is in line with its communication."

How to cite this chapter: Levallois-Barth C., Chauvet D. "Certifying for compliance: implementing the policy framework and beyond", *in Signs of trust – The impact of seals on personal data management*, Paris, Handbook 2 Chair Values and Policies of Personal Information, Coordinated by Claire Levallois-Barth, January, 2018, chapter 6, pages 91–113.

http://www.personal-information.org/

Chapter 7.

Certifying for credibility: from current practices to quality improvement

Claire Levallois-Barth

7

While CNIL Privacy Seals and EuroPriSe are aimed to reach compliance with more than just legal obligations (see Chapter 6), some external signs of trust are part of a different approach: gaining trust through certification credibility (7.1.). These signs are issued by private service providers on a very competitive market, where applying organisations face fragmented supply, unknown to consumers (7.2.). Furthermore, some of these seals could potentially mislead users and counter-productively entail mitigated reactions, or even mis-trust (7.3.).

7.1. Using credibility to gain trust

In one of the interviews carried out for the purposes of this handbook from October 2015 to September 2017, one person stressed that "*users gain trust not necessarily through an act or a legal framework, of which the final user isn't even aware.*"

The sign of a proactive engagement on data protection

Searching for credibility may also aim to correct information asymmetry[1] as companies share their data protection policy and the measures taken to implement it with consumers. As regards certification, this search should go further than a mere marketing statement, which can be unconvincing and even counterproductive, and should provide sufficient guarantees in practice.

1 Information asymmetry is addressed at the beginning of Chapter 9.

Certifying for credibility: from current practices to quality improvement

Words of a trusted third party

"Certification is a quality and commercial process. It has nothing to do with compliance. It does not guarantee compliance; there are other ways of dealing with compliance."

Certification is voluntary, which means some measures — or as some would say, minimal requirements — are implemented internally, then assessed by a third party. This does not prevent the misuse of personal data, yet ensures certified organisations are willing to work on data protection and use it as a selling point.

In this respect, certification organisations express a clear commitment towards their clients, stressing certain points to ensure long-term brand credibility. This credibility relies on more than mere compliance, which means that minimum commitments must go beyond mere compliance as well. Organisations establish a communications strategy that shows they embrace in a very practical way some technical or legal standards, values and ethical principles. Such strategy is therefore quite similar to a sustainable development and corporate social responsibility approach.

Words of an expert from a certification organisation

"Certification guarantees best-effort service. It means you are not perfect, but you have the necessary resources for course correction… You have to prove that you're at least trying."

Criteria are written in such a way as to be understood by a majority, focusing on the daily life of company and users: best practices implemented for cloud services (e.g. the requirement that data are to be stored in Europe only), guarantees related to algorithms or to certain kinds of personal data (data related to children, data on health), the use of technologies that reinforce privacy protection such as anonymisation techniques, participating in opt-out systems for direct marketing.

Certification thus seems to be one of many available marketing strategies. Some organisations have chosen other signs of trust, including:

- pure declaration, by sharing their "Commitment to transparency",[2] adopting their own data protection charter,[3] or committing to a code of conduct;[4]
- bringing awareness to Internet users on risks related to personal data and helping them take (back) control of their digital identity;[5]
- helping build a trusted ecosystem by providing third-party app developers with technical tools so that the apps inform end users on the personal data flow that is created;[6]
- committing to compliance with legal provisions and adopting Binding Corporate Rules approved by supervisory authorities.[7]

Others merely choose not to provide guarantees and set more attractive prices instead.

2 AXA, Commitment to transparency, https://group.axa.com/en/about-us/data-privacy

3 Orange's Charter on Data Protection and Personal Privacy - January 2010 (Updated in December 2014), https://bienvivreledigital.orange.fr/mes-donnees-mon-identite/charte-protection-desdonnees-personnelles-et-de-la-vie-privee; Crédit Agricole, Charter on Personal Data, https://www.credit-agricole.fr/nos-engagements/charte-des-donnees-personnelles.html

4 Cloud Infrastructure Services Providers in Europe (CISPE) Code Of Conduct, meant to prepare for the enforcement of the EU's GDPR, https://cispe.cloud/code-of-conduct/

5 MAIF, mesdatasetmoi, https://www.mesdatasetmoi.fr/

6 Orange Trust Badge, https://partner.orange.com/trust-badge/

7 HP, *Qu'est-ce que les BCR HP ?*, http://www8.hp.com/fr/fr/binding-corporate-rules.html

One asset of certifying for credibility is that it is likely to prompt internal dynamics more easily than certifying for compliance, which is more demanding and less adapted to the organisational culture. Choosing to get certified is a structuring decision for the organisation; it is often made at the executive management level and implementing it has an impact on many different roles and services along the data processing chain (information systems, law, marketing, audit, compliance, quality, etc.) and involves employees as well.

Assessment allows to identify strengths and weaknesses, thus possibly resulting in measures to improve internal personal data governance.

A possible leverage effect: the improvement process

The very existence of an improvement process shows the approach is not only regulatory, but part of a risk management system involving both the data controller and the data subjects. AFNOR Normalisation, the French national organisation for standardisation, especially advocates "*a risk-based approach, which [...] is part of an iterative continuous improvement process in terms of security and data protection.*"[8]

Certification organisations have therefore started to promote commercial offers to help companies identify risks, take adapted action to mitigate them and guarantee improvement to users.

The Cloud Seal is representative of such strategy, even though its criteria do not solely focus on data protection but rather on information security, following Standard ISO 27001. It provides three different levels of guarantee:

- **Initial level:** The applicant's self-assessment is checked by an expert, who may request any information or document as evidence of the assessment;
- **Advanced level:** The company is required to provide a list of documents and the expert may request any additional information or documents from the applicant;
- **Expert level:** The company receives on-site audit by an auditor and its clients assess the services it provides.

8 AFNOR *Normalisation, Guide Protection des données personnelles : l'apport des normes volontaires*, January 2017, p. 6, http://normalisation.afnor.org/wp-content/uploads/2017/02/AFNOR_Guide_Protection_des_donnees_perso_HD.pdf

According to the level, a seal may be delivered for 2 years (initial level), 3 years (advanced) or 4 years (expert). When applying for the first time, companies may select the level they want. When reapplying, they may keep the same level or select a higher one. If they ask for the same level, they need to get a higher score than the one they got for the previous certification. If they ask for a higher level, requirements are stricter regarding both the final average of scores and the minimum score required for each criterion.

The ADEL Label also uses a marking system, which scores and rates several different categories and delivers recommendations and guidance.[9]

For its part, Bureau Veritas believes "*it is hard to see how companies would be able to claim with 100% certainty that their actual privacy protection is failsafe across all of their systems and databases everywhere, including in subsidiaries.*"[10] The certification organisation has thus announced its intention to use "*a certification system*" awarded on "*three levels that allow businesses to be certified based on the maturity of their process*":

- the "*privacy-by-design checked product/service*" certification would allow the organisation to engage in a compliance process for a specific product or service "*for using a specific product or service design, a data architecture, and de-identification or similar methods.*" That label would "*let businesses begin the privacy certification process without redoing their entire IT architecture;*"
- the "*Governance*" certification would be part of a wider quality process in which the organisation could certify its data management system;
- the "*GDPR*" certification would offer voluntary certification of compliance and be awarded based on guidance derived from the regulation. It would let the organisation show they are compliant with the legislation (see Chapter 8).[11]

9 ADEL Label, Algorithm Data ETHICS LABEL, http://www.adel-label.com/label-adel/

10 Bureau Veritas, Restoring trust in Big Data, November 2016, http://www.move-forward-with-privacy.bureauveritas.com/wp-content/uploads/2016/11/Bureau-Veritas-brochure-english-privacy-2016.pdf

11 This project materialised in the Technical Standard related to personal data protection in compliance with the regulation (EU) 2016/679, published in October 2017, http://www.bureauveritas.com/home/news/business-news/worlds-first-personal-data-protection-standard

However, companies that wish to apply for "quality" certification are currently having trouble finding seals tailored to their needs. Some even give up on certification in spite of the high market competition.

7.2. A very competitive market

As part of their self-regulation process, companies face a supply that is both fragmented and not publicly well-known. As Bureau Veritas puts it, "*the multiplicity of labels can easily have the opposite effect: instead of restoring trust, it can lead to confusion.*"[12]

Fragmented supply

In France, the market is mainly meant to meet the needs of certain professions or re-assure on the use of certain technologies. Neither the *Fédération Nationale des Tiers de Confiance*'s (FNTC) E-vote Seal or ADEL's label have been issued so far. France IT's Cloud Seal was granted to nine entities and the Cloud Confidence Seal to two companies (see table on following page). Therefore, few seals are awarded to organisations. One explanation could be the strong competition taking place among service providers.

Words of a lawyer

"Competition is ruining the market in the private sector. Companies that created a certification put in a lot of work before presenting their first clients with offers; they invested a lot. Yet, if they merge with a competitor that has a higher business development capacity, the competitor will most likely take the lion's share and they will only get bits and pieces."

12 Fragmented supply

Organisation	Seal name	Field	Criteria	Year of creation	Number of seals issued
Adel	ADEL (*Algorithm Data Ethic Label*)	Services / Algorithms	Ethical rules	2016	0
Cloud Confidence	Certification Cloud Confidence	Services / Cloud	Legal standards + best practices for information security	2014	2
FEVAD (Federation of E-commerce and Distance Selling)	FEVAD Trust Mark	Services / E-commerce	Legal standards + FEVAD's Ethical Rules for E-commerce and Distance Selling	1957	400+
FNTC	E-Vote	Services / E-vote	CNIL guidelines on security requirements for Internet voting	2016	0
France IT	Label Cloud	Services / Cloud	200 best practices for Cloud	2012	9

Table 9. "Quality" seals issued by French private organisations

For instance, the Website Seal, launched in 1999 by the *Fédération du e-commerce et de la vente à distance* (FEVAD) and the *Fédération des entreprises du commerce et de la distribution* (FCD) for websites, was never actually created even though its 27 requirements were drawn up with the help of the French General Directorate for Competition Policy, Consumer Affairs and Fraud Control (DGCCRF) and the CNIL. A trusted third party we interviewed believes this might be because companies that were already widely known did not feel the need to get certified as they were already members of professional federations and followed their ethical rules. Thus, they preferred to only be awarded the FEVAD trust mark. The Website Seal could have been interesting for smaller enterprises that wished to get more recognition; they still gave up on it as it required too much of a financial effort: a third-party certifier had to be paid, on top of the €1,000 FEVAD membership fee.

In the field of cloud computing, a first explanation is that two French seals are competing, not mentioning the CISPE (Cloud Infrastructure Service Providers in Europe), a European initiative launched in 2016 that gathers around twenty Cloud Infrastructure Providers from fifteen countries.

A second explanation lies in the nature of the stakeholders involved. Cloud Seals are held by French organisations and companies; while the Cloud market is mostly made up of American providers (Amazon, Google, IBM, Microsoft, Oracle, Salesforce…) that do not support such initiatives, therefore limiting their scope. Google in particular refuses to specify data location.

The FEVAD trust mark for distance selling, created in 1957, stands out by the number of organisations it has certified, around 400. This is not specific to France. All around Europe, e-commerce trust marks gather many more members. In that field, clients' trust relies mainly on data protection, as well as on guarantees related to delivery, product return, replacement or repair. These marks allow for heterogeneous data protection levels, as legal obligations differ according to the country, as do the goals pursued by the professional organisation issuing the certification. Besides, they raise members' awareness.

- FEVAD's Ethical Rules for E-commerce and Distance Selling pinpoint the main legal provisions and require member companies to maintain and abide by two opt-out lists, a telephone preference list and a mailing preference list called "*Robinson List — Stop Publicité*".

- The Spanish trust mark Confianza Online is one of such providers of concrete signs of trust. Its 32-page Ethical Code was officially approved by three public organisations: the Spanish Data Protection Agency, the National Consumer Institute, and the Ministry of Industry, Tourism and Trade.

These marks created partnerships at the European level, where the main competition opposes two organisations with similar ambition: the European Multichannel & Online Trade Association (EMOTA) and Ecommerce Europe.

- The European association Ecommerce Europe gathers 25,000 companies and 19 national associations, including FEVAD from France (400 members), BeCommerce, Belgium; Thuiswinkel, Netherlands (2,217 seals); E-Maerket, Denmark (2,200 labels). It awards the ECommerce Europe trust mark to 10,000 online shops for free.[13] The trust mark should be displayed together with a certified national mark. Companies that are granted the mark are required to comply with the Ecommerce

13 https://www.ecommerce-europe.eu/ecommerce-europe-trustmark/

Europe Code of Conduct — which is pretty basic as regards data protection, to say the least[14] — and that of the national association, based on national laws;

- Similarly, only companies certified with a national seal partnered with the EMOTA may display the EMOTA seal on their website.

Attractive prices

Prices vary according to the certification scope and criteria, yet mostly depend on the applying company's size and annual turnover:

- FEVAD membership fees depend on turnover; with annual fees from €1,000 up to €35,000;
- Belgian BeCommerce certification costs €500 to audit a first website for certification, then €200 for other websites, on top of the association's membership fees that range from €150 to €11,000 when turnover exceeds €25 million;
- Confianza Online's annual fees start at €295 (VAT excluded) for companies with a turnover of less than 1 million euros and can go up to €3,500 (VAT excluded) for companies with a turnover higher than €25 million;
- the Cloud Seal varies from €1,000 to €5,500 (VAT excluded), depending whether the applicant is a member of France IT and which certification they are requesting;
- Cloud service declaration under the CISPE (Cloud Infrastructure Service Providers in Europe) code of conduct amounts to €990 for the declaration of one service and €2,990 for the declaration of three services or more.

The same logic applies for American seals:

- getting the TRUSTe certification costs $399 if turnover is less than $500,000 and $8,999 if turnover exceeds $2 billion;
- getting the BBBonline certification costs $200 if total sales are less than $1 million and $6,000 if total sales are equal or higher to $2 billion.

Getting certified for the first time is often more expensive. BeCommerce certification fees are €550 for the first seal and €300 for two-year renewal.

---

14 https://www.ecommercetrustmark.eu/the-code-of-conduct/, of which the only part on data protection states: "*We respect your privacy, protect your data and care for a safe web-environment. We are transparent and inform you about the collecting and processing of your data and the purposes for which we use them, including information regarding cookies policy. Data is collected to carry out the contract and to improve our offer to you and your buying experience. Your data is collected in compliance with data protection and privacy legislation and, as far as legally required, only with your explicit consent.*"

According to a trusted third-party, a €10,000 fee is too high for small and medium enterprises, which are willing to invest €5,000. Such numbers obviously depend on what benefits the company is trying to achieve through certification. A lawyer mentioned the example of a start-up company that did not mind paying €40,000, as it was developing a technology that was "*very harsh on personal data*" and trying to reassure both investors and clients.

In some cases, fees do not reflect the actual cost that auditors should charge. According to a trusted third party, auditors offer "*very reasonable*" prices to first attract clients and begin a commercial relationship, then charge further services as part of an improvement process.

Meanwhile, audit automation tools are emerging. Machines and algorithms allow to carry out automated evaluations, thus reducing their costs. For instance, StarAudit charges €400 for self-assessment and report publication.

Data protection certification has therefore become an economic activity that attracts many service providers. "*As a result, it appears there is a certain ambivalence to certification. Indeed, in the classical fields where feedback can be gathered, it appears that certification practices that are not compliant with consumer protection and harmful to competition still exist.*"[15]

7.3. The misleading effect

A quality-based approach is likely to confuse and mislead users.

On the one hand, quality-based criteria can be of any level. One can gladly notice they usually include the main data protection obligations (lawfulness, proportionality, purpose limitation, transparency) included in Directive 95/46/EC and, starting May 25, 2018, in the General Data Protection Regulation (represented in the diagram below under GDPR_OB). The guarantees brought by certification derive from these requirements (GPDR_OB1,

15 Penneau, A. (2014). *Certification et codes de conduite privés : article 38 et 39 (dans leur version originelle), in La proposition de règlement européen relatif aux données personnelles : propositions du réseau Trans Europe Experts, sous la direction de Nathalie Martial-Braz, Société de législation comparée*, volume 9, 2014, p. 351

GPDR_OB2); yet they do not mean that compliance with other legal obligations has been assessed (GPDR_OB3, GPDR_OB4).

"Quality" requirements (represented in the diagram below under Q_RE) do not fall in the area of legislation *per se*; they hardly provide points of comparison between the various criteria. For instance, there can be requirements on opt-out list membership and practical modalities (Q_RE1); on hosting data in the EU (Q_RE2); on appointing a Data Protection Officer in cases where it is not legally mandatory (Q_RE3); or simply on the establishment of a business policy (Q_RE4).

This guarantees that experts simply assessed the company has properly implemented best practices in order to meet requirements. Data protection governance certification classically means compliance with quality-based procedures, and does not guarantee the quality of the data processing — even if it helps.

► A good example is the American TRUSTe certification, which certifies the existence of a company's business policy, but not its quality.

Words of an expert from a certification organisation

"We focus on best practices mostly. We choose to have limited requirements that focus on the existence and proper implementation of a business policy. We look for substance behind the commitment. It's the Anglo-Saxon way."

On the other hand, time is a relevant variable as well. Evaluations are carried out at T0 over a period of one to five years. There are usually very few ex post investigations during that period. Indeed, little information can be found on whether existing certification is followed up on, even though the assessed products, services and governance rules probably have evolved since then. Certification organisations that do provide for check-ups do not seem to give information on how they are actually implemented, so one can wonder as to whether they are done in practice. Investigations are mostly carried out for renewals. Such ambiguity especially arises for e-commerce trust marks, as compliance can be assessed with varying levels of regularity — from renewal periods to sporadic and continuous checks.

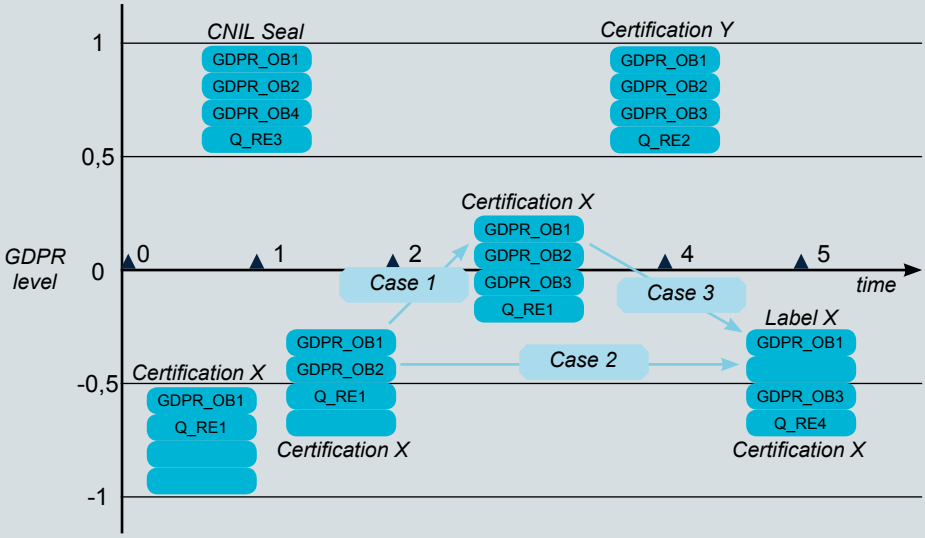


Figure 1. Confusing effects

► The regulation of Belgian BeCommerce certification states that "*at the beginning of every year, 20% of companies that hold quality certification and are thus bound by BeCommerce's certification regulations, will be randomly selected by a bailiff and undergo a control certification procedure. Such certifications will take place over the whole year and will obviously be surprise checks for the companies in question.*"[16]

Certification requirements also usually vary over time, as global protection levels can increase or decrease according to whether certain requirements are cancelled, or more subtly, amended.

16 https://www.becommerce.be/upload/Label_FR_Reglement201420140313144711.pdf

Public information is also a requirement for credibility. It implies implementing conflict-resolution mechanisms in the interest of all parties, should a dispute arise between the certified company and the users whose data is used. Yet some seals, just like the CNIL Privacy Seals, only provide a contact email address with no further specification, while trust marks in the field of e-commerce and distance selling, such as Confianza Online, Trust Shops and ESRB, offer a mediation process and make it a significant part of their communications. The same goes for the Privacy Shield agreement, which provides no credible way of filling a complaint. The agreement did introduce an Ombudsperson Mechanism Procedure; yet its effectiveness and independence have yet to be proven.[17]

This particular problem is the result of some certification organisations' unwillingness and powerlessness to take redress action against their members (for associations) or clients (for private certification companies) in case of abuse. The announced sanctions include mere warnings, temporary suspensions, dismissals or financial penalties.[18]

Certification is hardly ever revoked, and when it is, it is never advertised — FEVAD specifies that sanctions are not made public — even though revocation is meant to act as an incentive to comply with commitments. When TRUSTe revoked its seal from Gratis Internet of Washington in 2005 for violating the policy on the protection of children's information, it did not disclose the nature of such violation, supposedly due to a confidentiality agreement.[19] Yet, as a lawyer pointed out, "*punishing bad behaviours seems to be a requirement for the credibility and longevity of certification.*"

However, in a competitive environment, service providers first need to certify a minimum number of clients, which implies widely accepting applicants to make up a first customer database. Only then, once the organisation has enough certified clients, can it consider strengthening requirements and punishing low achievers.

---

17 See MEP Claude Moraes's speech from the Personal data in international treaties and agreements: Privacy Shield Symposium of the Chair Values and Policies of Personal Information: https://cvpip.wp.imt.fr/2017/02/06/privacy-shield-claude-moraes-speech/

18 European Parliament, Directorate General for Internal Policies, A Pan-European Trustmark for E-Commerce: Possibilities and Opportunities, study, IP/A/IMCO/ST/2012-04, July 2012, http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/492433/IPOL-IMCO_ET(2012)492433_EN.pdf

19 Associated Press, 'Privacy-Assurance Seal Yanked', Wired, 2 September 2005, http://www.wired.com/techbiz/media/news/2005/02/66557

As data protection certification faces the risk of being dumbed down, the issue is now to reflect upon the regulations that should be passed to provide a framework regulating the market and under which modalities. The GDPR leaves space for several options in this respect (see Chapter 8).

In the United States

US lawmakers prefer self-regulation by the market; therefore, there are many, mostly private, labels and trust marks. There is no general legal framework in the United States like there is in the EU, but still a few sector-specific federal laws.[20] Some states, such as California, have more demanding laws or have made breach notification mandatory.[21] Lawmakers are therefore only involved in specific fields and for specific uses. Indeed, as Isabelle Falque-Pierrotin, CNIL Chair, explained during a meeting hosted by the Chair Values and Policies of Personal Information on January 8, 2016,[22] "*data protection is closely linked to countries' cultural sensitivities: we [Europeans] believe data protection is a fundamental right while the United States focus rather on consumer protection.*" [Unofficial translation from the original French]

The Federal Trade Commission (FTC) is responsible for consumer protection and the prevention of anticompetitive practices. In this respect, it is involved in data protection,[23] requiring companies to put an end to their illegal practices and, when needed, taking coercive action.

- The FTC may require organisations to implement clear data protection and security policies or erase illegally obtained consumer data. In 2011, it compelled Facebook to inform consumers and obtain their affirmative express consent before enacting changes that override their privacy preferences.

---

20 Such as the 1974 Privacy Act on the collection, maintenance, use, and dissemination of personally identifiable information about individuals by federal agencies, the 1996 Health Insurance Portability and Accountability Act (HIPAA), the 1998 Children's Online Privacy Protection Act (COPPA) about children under 13 years of age, and the 1999 Gramm-Leach-Bliley Act on financial services.

21 The California Online Privacy Protection Act of 2003 — Business and Professions Code requires commercial websites and online services to include a privacy policy on their website. Nebraska and Pennsylvania also have specific laws prohibiting knowingly making a false or misleading statement in a privacy policy.

22 Chair Values and Policies of Personal Information, 10th Symposium on Personal Data in the International Treaties and Agreements, 8 January 2016.

23 Especially in the enforcement of sector-specific laws such as the 1970 Fair Credit Reporting Act or the COPPA. In particular, section 5 of the Federal Trade Commission Act prohibits unfair or deceptive practices.

- The FTC may also require companies to have annual evaluations carried out by independent experts or pay monetary remedies to consumers.

Non-compliance with FTC orders may lead the Commission to seek financial penalties. Not only do fines affect companies' brand image, they also have a significant deterrent effect. In 2012, after a series of talks with the FTC, Google had to pay $22.5 million to settle charges for tracking users of the Safari Internet browser.[24]

In cases such as this one, certification based on self-assessment only ensures users that the website openly shares its privacy policy. That policy may specify how information is collected, used and shared and how users may exert a measure of control on their personal data. Such display is thus meant to inform users and allow them to make an informed choice on how their data is used. Worldwide companies such as Apple, eBay, The New York Times, Cisco, Disneyland, EA Games, Hewlett Packard, IBM, McDonalds, Oracle and Verizon are all certified. Some of them even have several seals.

Yet in the United States, privacy protection organisations are questioning the value of such trust signs. Privacy International, for one, believes they often only convey "*an illusion of privacy protection*" without delivering anything additional to legal obligations.[25]

A good example is the American TRUSTe certification, largest Privacy certification provider, that takes part in self-regulation mechanisms implemented by the Children's Online Privacy Protection Act (COPPA), the Safe Harbour and Privacy Shield agreements between the EU and the United States,[26] and the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules. The non-profit organisation, that employed 80 people and

---

24 Also, in 2013, social network Path had settled FTC charges by agreeing to pay a $800,000 fine (about €588,000 at the time) and to submit to privacy audits. In 2014, Yelp had to pay a $450,000 penalty due to the collection of the personal information of children under 13 without first notifying parents and obtaining their consent.

25 Privacy International, 'Response to the European Commission's Communication on the 'Comprehensive Approach on Personal Data Privacy International, January 2011, p. 11 http://ec.europa.eu/justice/news/consulting_public/0006/contributions/organisations/pi_en.pdf: "*We have strong reservations about the value of 'privacy seals', which can often create an illusion of privacy protection without delivering anything additional to legal obligations, and we especially question the value of privacy seals operated by for-profit companies when the profits of the seal program are wholly dependent on the revenues from seal holders.*"

26 On August 16, 2016, TRUSTe announced it was working with over 500 companies to assess and verify compliance with the new requirements for the EU-U.S. Privacy Shield and provide dispute resolution services; https://www.trustarc.com/press/500-companies-working-truste-comply-eu-u-s-privacy-shield/.

had 4,000 customers, carried out poor checks the holders of its certification. In June 2000, the FTC thus sued the certified company Toysmart.com for violating its privacy policy and selling customer information.[27] Other companies were also sued for the same kind of violation.

- In 2007, a study showed that Microsoft, Yahoo, Chase Manhattan Bank and Geocities, all holders of TRUSTe certification, carried out questionable privacy policies on their websites. The same went for Equifax, holder of a BBBOnLine seal.[28]

- Another study, carried out by Carnegie Mellon University, exposed that the Facebook, MSN and AOL websites, all holders of the TRUSTe EU Safe Harbour Privacy Seal, misused the Platform for Privacy Preferences (P3P). Out of 2,417 TRUSTe-certified websites, 134 had invalid cookie compact privacy policies, among which 21 were part of the first 100 most popular websites.[29]

TRUSTe also was subject to sanctions, including a $200,000 penalty by the FTC in November 2014, for misleading practices: from 2007 to 2013, it tacitly renewed certification for 1,000 companies without conducting ex post evaluations.[30]

TRUSTe's name change thus does not come as a surprise. The organisation is now called TrustArc, officially with a view to "*reflect [its] transformation from a certification company into a global provider of technology powered privacy solutions.*"[31]

---

27 FTC v Toysmart.com, LLC, and Toysmart.com, Inc., District of Massachusetts, Civil Action No. 00–11341-RGS, https://www.ftc.gov/enforcement/cases-proceedings/x000075/toysmartcom-llc-toysmartcom-inc.

28 LaRose, R. and Rifon, N., (2007). Promoting i-Safety: Effects of Privacy Warnings and Privacy Seals on Risk Assessment and Online Privacy Behavior (Summer 2007), vol. 41, Journal of Consumer Affairs 12.

29 Leon, P. G., Faith Cranor, L., McDonald, A. M., and McGuire, R., (2010). Token attempt: The Misrepresentation of Website Privacy Policies Through the Misuse of P3P Compact Policy Tokens, CyLab. Paper 73, http://repository.cmu.edu/cylab/73. See also Connolly, C., Greenleaf, G. and Waters, N. (2014). Privacy self-regulation in crisis? TRUSTe's 'deceptive' practices, 132 Privacy Laws & Business International Report, 13-17, December 2014.

30 FTC Approves Final Order In TRUSTe Privacy Case, https://www.ftc.gov/news-events/press-releases/2014/11/truste-settles-ftc-charges-it-deceived-consumers-through-its

31 The Leader in Privacy Compliance and Risk Management Solutions Has a New Name — TrustArc, https://www.trustarc.com/about/.

TrustArc provides several TRUSTe seals and sells solutions to manage compliance with the European legal framework, namely the GDPR and Privacy Shield. Should that kind of market activity, in keeping with the developing market of data protection certification providers, be regulated to reduce abuse? If so, how? What solutions does the GDPR bring to such issue?

How to cite this chapter: Levallois-Barth C. “Certifying for credibility: from current practices to quality improvement”, *in Signs of trust – The impact of seals on personal data management*, Paris, Handbook 2 Chair Values and Policies of Personal Information, Coordinated by Claire Levallois-Barth, January, 2018, chapter 7, pages 115–132.

http://www.personal-information.org/

«Assemblée» — Thierry Citron

Chapter 8.

Certification mechanisms in the General Data Protection Regulation (GDPR)

Claire Levallois-Barth

8

On April 27, 2016, the European Union passed Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC (General Data Protection Regulation, or GDPR).[1] The text entered into force on May 25, 2016 and will be applicable starting May 25, 2018. After that date, the French Data Protection Act (*loi Informatique et Libertés*) should be largely amended.

Consistent with European Directive 95/46/EC (Data Protection Directive),[2] the GDPR takes over the existing protection principles (lawfulness, fairness, transparency, purpose limitation, data minimisation and accuracy, limited storage periods, adequate level of protection for cross-border flows of data, increased protection of sensitive data, etc.) while adding new obligations (right to personal data portability, right to be forgotten in the online environment, etc.).[3]

1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), EUOJ, L 119, 4.5.2013, p. 1.

2 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, ECOJ, L 281, 23.11.1995, p. 31.

3 See Levallois-Barth, C. (2017). Personal Data: A European Reform For A Digital 21st Century, Revue TELECOM 185, June 2017.

Certification mechanisms in the General Data Protection Regulation (GDPR)

New features include the possibility for "*data protection certification, seals and marks*." The GDPR uses these three terms: ***certification***, ***seal*** and ***mark***. The point here will be to make out if there actually is a difference between these three notions, and if so, to define it.

The Regulation classically pictures certification as a sign of compliance, which could materialise as a seal. It provides that "*where the criteria are approved by the Board [European Data Protection Board, or EDPB], this may result in a common certification, the European Data Protection Seal.*"[4]

As far as the term of "mark" and the confusion such a term can bring about are concerned, there are two possible interpretations. The first is that its use could be seen as a will to allow for a possible inclusion of signs of trust in the European trademark system.[5] In France, for instance, it is a registered trademark which protects the rights of third parties authorised to use these marks. Legal recognition confers the mark owner the exclusive right to use the mark; an unauthorised and unfair use can lead to civil action for trademark infringement.[6] According to the second interpretation, and in light of certain propositions made during the negotiations on the Regulation, we may infer the difference between "data

4 Art. 42-5, GDPR.

5 See Lachaud, E., (2016). Why the certification process defined in the General Data Protection Regulation cannot be successful. Computer Law & Security Review 32, 814–826.

6 Art. L. 716-1, French Intellectual Property Code.

protection seals" and "marks" is purely rhetorical.[7] Indeed, the European Parliament related both notions when it suggested that "*supervisory authorities shall grant [...] the standardised data protection mark named 'European Data Protection Seal'.*"[8] In practical terms, we can notice that GDPR articles 42 "Certification" and 43 "Certification bodies" focus on certification only in their titles.

More precisely, Article 42 mentions the purpose of certification, which it describes as a tool for demonstrating compliance (8.1.). Yet, the modalities of issuing certification, seals or marks are not entirely known, since the GDPR includes several options (8.2.) and hints at several prospects for its implementation (8.3.).

8.1. Certification mechanisms: a means to demonstrate compliance with legislation

Seals, along with data protection certification and marks, allow an entity to prove — under rebuttable presumption — it has implemented appropriate and efficient measures to comply with the legislation.

This contributes to one of the GDPR's new obligations, the "accountability" principle, according to which organisations should "*implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with [the] Regulation.*"[9] The goal is to ensure the entity collecting and processing personal data has implemented practical tools in order to ensure effective data protection.[10]

7 See, Lachaud, E., (2016). Why the certification process defined in the General Data Protection Regulation cannot be successful. Computer Law & Security Review 32, 814–826.

8 European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), art. 39 1e.

9 Art. 24-1, GDPR.

10 See Article 29 Data Protection Working Group, Opinion 3/2010 of 13 July 2010 on the principle of accountability (WP173), p. 3.

The accountability principle

The accountability principle was explicitly recognised in the Organisation for Economic Co-operation and Development's (OECD) 1980 Guidelines on the Protection of Privacy. Point 14 specifies on that account: "*Accountability Principle: A data controller should be accountable for complying with measures which give effect to the principles stated above.*" It is one of the main concepts of the Asia-Pacific Economic Cooperation (APEC) Privacy Framework (point 26). It is also included in the latest draft for ISO Standard 29100 which establishes a privacy framework.

These tools can especially be used to apply a data protection policy, an approved code of conduct or approved certification mechanisms. Certification is therefore not mandatory; rather, choice is left to the data controller, according to specific data processing circumstances, whether to demonstrate they have taken appropriate and efficient action to comply with legislation. In particular, certification schemes include compliance with two requirements: the traditional security of processing and the new obligation to ensure data protection by design and data protection by default.[11] Certification also allows controllers to demonstrate they used a processor providing "*sufficient guarantees.*"[12] Finally, certification also steps in during the imposition of sanctions, since supervisory authorities have to take it into account to decide, where appropriate, whether or not to impose administrative fines as well as the amount of such fines.[13]

This simple presumption system is designed as a tool which should:

- provide legal certainty for controllers by allowing them to demonstrate that the personal data they transmit to other controllers have been legally collected and can be legally used;.
- display the level of protection of their data to users and consumers.[14]

Transparency is enhanced both for the individuals involved (business-to-consumer, or B2C) and for the data controllers (business-to-business, or B2B). It is therefore increased

11 See *« Identités numériques », Cahier n°1*, Chair on Values and Policies of Personal Information, coordinated by Claire Levallois-Barth, p.67

12 See recital 81 and art. 28-5, GDPR.

13 Art. 83-2(j), GDPR.

14 Recital 100, GDPR.

all along the life cycle of personal data, from their collection to their processing, including when data controllers share them with processors.

Certification is indeed addressed to controllers and processors, whether they fall within the scope of the GDPR or not. This is an important aspect: the Regulation gives EU-established organisations the right to legally transfer personal data to a certified organisation, even if this organisation is established in a country that does not have an adequate level of protection. This mechanism allows to ***export the European standard*** on data protection globally, and should allow non-EU companies to enter the EU market more easily.

Transfer of personal data outside the European Union (GDPR Articles 45 and 46)

The GDPR, like Directive 95/46/EC, provides that a transfer of personal data outside the European Union may only take place to a third country, a territory or one or more specified sectors within that third country, or an international organisation, that ensures an adequate level of protection. The level of protection is recognised by the European Commission, which published adequacy decisions. In the absence of an adequacy decision, the controller or processor can transfer data if they provide for "*appropriate safeguards*."

These safeguards may consist of Binding Corporate Rules, contractual clauses, an approved code of conduct or an "*approved certification mechanism […] together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights*." Safeguards may also include an international agreement, like the EU-US Privacy Shield agreement concluded in July 2016, even if its implementation is now under political and legal challenge.[15]

15 See Levallois-Barth, C., Meseguer, I. (2016). *Privacy Shield : un bouclier à peine brandi déjà ébréché ?*, Editorial to trimestral Newsletter No 5, Chair on Values and Policies of Personal Information, December 2016.

8.2. Implementing options

The GDPR was written to be flexible, allowing all existing certification schemes to coexist, be they public seals issued at the national or EU level or seals issued by associations or private bodies. Certification bodies will need to get an accreditation, which they can be granted through various ways.

Seals are issued either by public authorities or private bodies

According to the rules set by the GDPR, a seal shall be delivered on the basis of criteria approved and published by the competent supervisory authority, on its territory (in France, the *Commission Nationale de l'Informatique et des Libertés* or CNIL).[16] Criteria can also be approved by the European Data Protection Board (EDPB).[17] In such case, this may result in a common certification, the European Data Protection Seal.[18] However, the GDPR does not specify how criteria will be defined and especially does not provide for the consultation of stakeholders (businesses, non-governmental organisations…), unlike its provisions towards a code of conduct.[19] This kind of consultation, which was proposed by the European Parliament at first reading, is however an established practice in the field of certification.

In order to receive a valid seal for a maximum and renewable period of three years, a controller or processor may address a supervisory authority or private entity such as AFNOR Certification, the British Standards Institution or Bureau Veritas. Both public and private entities will be able to issue seals on the basis of criteria approved at the national level (by the supervisory authority) and the EU level (by the EDPB).

Possibilities will therefore include:

- a label established at the EU level and issued by a national supervisory authority;
- a label established at the EU level and issued by a private certification body;

16 Art. 58-3(f), GDPR.

17 The EDPB will consist of the head of a supervisory authority of each Member State and the European Data Protection Supervisor or their respective representatives, and should have legal personality and increased powers.

18 Art. 42-5, GDPR.

19 See Recital 99, GDPR. "*When drawing up a code of conduct, or when amending or extending such a code, associations and other bodies representing categories of controllers or processors should consult relevant stakeholders, including data subjects where feasible, and have regard to submissions received and views expressed in response to such consultations.*"

- a label based on national criteria and issued by a national supervisory authority;
- a label based on national criteria and issued by a private certification body.

Relying on both public and private entities shows there was a compromise: the European Parliament suggested that national supervisory authorities be the only entities to issue seals for data protection (also referred to in this handbook as "Data Protection Authorities") while the European Commission and the European Council preferred accrediting private auditors.

Competent supervisory authority (GDPR Article 56)

The competent supervisory authority is the supervisory authority of the main establishment or of the single establishment of the controller or processor. If the controller or processor has establishments in several Member States, their main establishment corresponds, in principle, to its central administration in the Union.
There are however exceptions to these principles.
As regards a controller: when the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, the establishment having taken such decisions is to be considered to be the main establishment;
As regards a processor: if the processor has no central administration in the Union, the establishment shall be where the main processing activities in the context of the activities of an establishment of the processor take place.

Nevertheless, the GDPR does not mention modalities for mutual recognition. It is not specified which status a competent supervisory authority in State A will grant a seal issued in accordance with the GDPR in State B by a competent authority or a private body.[20] The Regulation does provide, however, that seals as well as all certification mechanisms will be collated in a public register held by the EDPB.[21]

20 In Switzerland, Article 7 of the Ordinance on Data Protection Certification (DPCO) of 28 September 2007, entitled "Recognition of foreign data protection certification", specifies that recognition is carried out by the Commissioner, in consultation with the Swiss Accreditation Service.

21 Art. 42-8, GDPR.

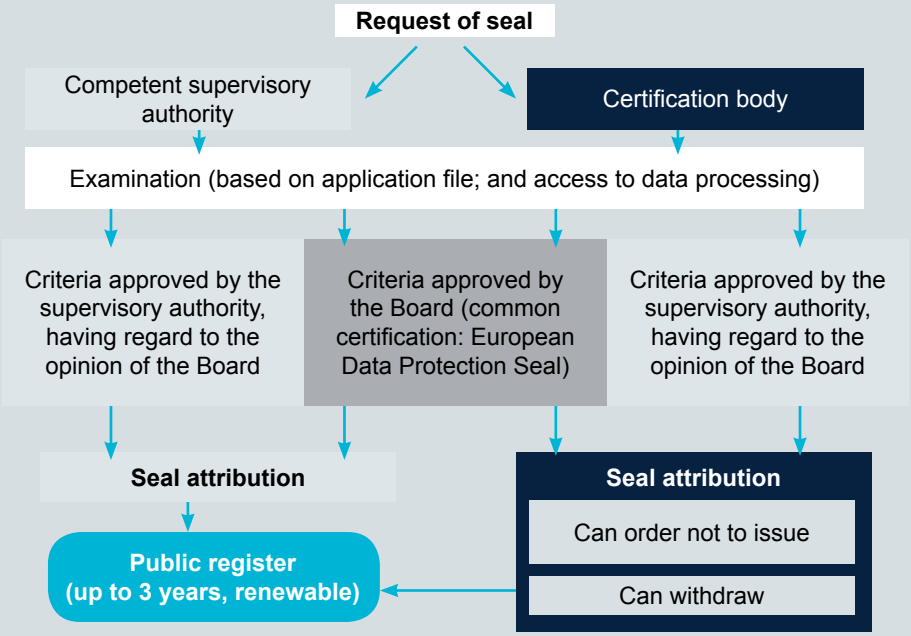


Figure 2. GDPR: Issuing a certification / seal

For seals issued by both public or private entities, the controller will have to provide all relevant information and access to its processing activities. In case the assessment is carried out by a certification body, that body will need to provide the supervisory authority with the reasons for granting the seal or, where appropriate, for withdrawing it. The authority will be able to withdraw a certification or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met.

It should be noted that the GDPR does not address the issue of the certification cost. However, the European Parliament had suggested to specify certification may be request-

ed "*for a reasonable fee taking into account the administrative costs,*" "*via a process that is transparent and not unduly burdensome" including "harmonised fees.*"[22]

As we have just explained, the harmonisation offered by the GDPR is far from complete; certification can be issued either by a supervisory authority or a certification body "*which ha[s] an appropriate level of expertise.*"[23] In such a case, the private entity will be "*under scrutiny.*"

Private certification bodies under scrutiny

The GDPR sets common criteria for certification bodies. It illustrates the general trend from "the current certification scheme to an interventionist stance aiming to push away the influence of certification bodies that are not competent, independent or impartial enough…"[24] As it is, it lets each State decide on how it wishes to monitor certification bodies. A body will therefore be accredited for a maximum period of five years:

- either by a national supervisory authority (in France, the CNIL — its authorisation powers will thus be reinforced);
- by the EDPB;
- or the national accreditation body.[25]

In that third case, the GDPR specifies that the national accreditation body will be "*named in accordance with Regulation (EC) No 765/2008 of the European Parliament and of the Council,*[26] *in accordance with EN-ISO/IEC 17065/2012*[27] *and the additional requirements established by the supervisory authority which is competent pursuant to Article 55 or 56.*" The French version of that body, the French Accreditation Committee (COFRAC), will as

22 Art. 39 1 sexies, 39 1bis and 1ter, "Certification", European Parliament legislative resolution of 12 March 2014, aforementioned.

23 Art. 42-5, GDPR.

24 Penneau, A. (2014). *Certification et codes de conduite privés : article 38 et 39 (dans leur version originelle), in La proposition de règlement européen relatif aux données personnelles : propositions du réseau Trans Europe Experts, sous la direction de Nathalie Martial-Braz, Société de législation comparée*, volume 9, 2014, p. 353. [Unofficial translation from the original French]

25 Art. 43-1 and article 70-1(o), GDPR

26 Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93, EUOJ, L 218, 13.8.2008, p. 1.

27 ISO/IEC 17065:2012 on Conformity assessment — Requirements for bodies certifying products, processes and service.

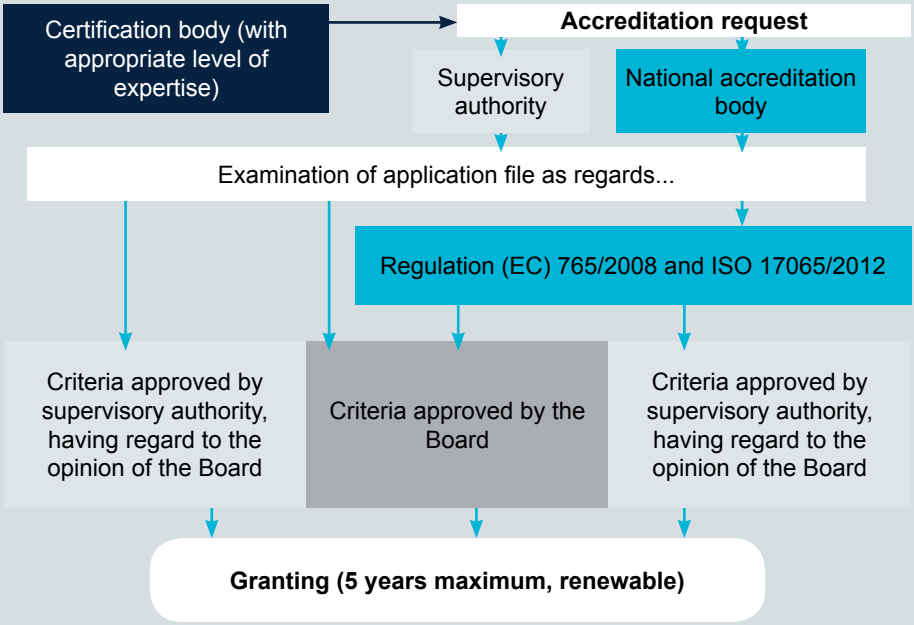


Figure 3. GDPR: Accrediting a certification body

usual have to comply with the requirements of an EU regulation, Regulation (EC) 765/2008, and, less commonly, of an ISO standard. This last condition is the most questionable, since ISO standards are by definition voluntary standards adopted through consensus in an international organisation, not an EU body.

Besides, Regulation (EC) 768/2008 requires that Member States appoint only one accreditation body so as to avoid competition. Yet the GDPR allows Member States to choose one of two options: a certification body can be accredited either by a supervisory authority or a national accreditation body. What criteria will guide their choice? This calls for careful action in that regard.

Whichever option is chosen, certification bodies will be accredited on the basis of criteria drafted and published by the supervisory authority, having regard to the opinion of the EDPB, or by the EDPB itself. They will be subject to institutional and procedural obligations. Not only will they need to commit to comply with the criteria approved by the supervisory authority or the EDPB, they will also have to demonstrate their independence and their expertise in terms of personal data protection, as well as the fact that their tasks do not result in a conflict of interest.

Besides, they will have to establish procedures for "*the issuing, periodic review and withdrawal of certification,*" the handling of "*complaints about infringements of the code or the manner in which the code [is being] implemented.*"[28] They will need "*to make those procedures and structures transparent to data subjects and the public.*" Only then will their name be included in the public register held by the EDPB.[29]

The competent supervisory authority or the national accreditation body will be able to withdraw accreditation if these conditions are not, or are no longer, met. If actions taken by the certification body infringe the GDPR, it might be subject, in addition, to an administrative fine up to €10 000 000, or in the case of a private body, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.1[30]

28 Art. 43-2, GDPR.

29 Art. 70-1(o), GDPR.

30 Art. 83-4b, GDPR.

8.3. Prospects for GDPR implementation and the role of public authorities

In all the ways we described, the GDPR therefore does not impose the establishment of data protection certification mechanisms or data protection seals and marks, but merely "encourage[s]" Member States, supervisory authorities, the EDPB and the European Commission in this effort.[31] Will they do it? More importantly, how will this "encouragement" materialise? In practical terms, the GDPR needs to be adapted into the secondary legislation, either at the national or the European level.

Working towards harmonised criteria

For now, the European Commission is assessing how relevant it is to adopt delegated or implementing acts.[32] Faced with inactivity on the business side, it has chosen to work on a common framework focusing on standardisation. As early as 2006, the Commission requested that the private sector "*work towards affordable security certification schemes for products, processes and services that will address EU-specific needs (in particular with respect to privacy),*" promoting a self-regulation approach.[33] As this did not stir any reaction, in 2010, it announced its intention to explore "*the possible creation of EU certification schemes (e.g. 'privacy seals') for 'privacy-compliant' processes, technologies, products and services.*"[34] Early 2015, it adopted a mandate for European standardisation organisations to draw up "*European standards and European standardisation deliverables for privacy and personal data protection management.*"[35] The mandate is focused on compliance with data protection by design and by default as well as security obligations.[36]

---

31 Art. 42-1, GDPR.

32 Such possibility is introduced in Articles 43-8 and 43-9, GDPR

33 Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of Regions, A strategy for a Secure Information Society – "Dialogue, partnership and empowerment", COM(2006) 251 final, Brussels, 31.05.2006, p. 9.

34 Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of Regions, A comprehensive approach on personal data protection in the European Union, COM(2010) 609 final, Brussels, 4.11.2010, p. 13.

35 Commission Implementing Decision of 20.1.2015 on a standardisation request to the European standardisation organisations as regards European standards and European standardisation deliverables for privacy and personal data protection management pursuant to Article 10(1) of Regulation (EU) No 1025/2012 of the European Parliament and of the Council in support of Directive 95/46/EC of the European Parliament and of the Council and in support of Union's security industrial policy, C(2015) 102 final, Brussels, 20.1.2015.

36 Annex to Commission implementing decision of 20.1.2015, C(2015) 102 final, aforementioned.

The European Committee for Standardization (CEN) and the European Committee for Electrotechnical Standardization (CENELEC) replied by creating a Joint Working Group on "Privacy management in products and services" (JW8).[37]

Meanwhile, the Article 29 Working Party (WP29), originally meant to adopt guidelines on certification by late December 2016, delayed their publication.

This is a complex issue, especially as only the French and German supervisory authorities have experience in the field of certification so far. Meanwhile, the British supervisory authority, the Information Commissioner Office (ICO), announced it was working on creating a privacy seal that will materialise as a trademarked logo.[38] Certification will be granted by private third parties accredited by the UK Accreditation Service (UKAS). Supervisory authorities therefore need to share more information in order to create shared practices. In practical terms, certification was one of the themes discussed at the first Fablab, organised by WP29 Chair on July 26, 2016. The 2016 Fablab, which contributed to the joint construction process, gathered around a hundred people — representatives from data protection authorities as well as civil society and the private sector — so as to stimulate ideas.

Adopting WP29 Guidelines

In order to clarify how the GDPR should be implemented, WP29 draws up guidelines using an unusual method. It selects working themes, then holds a public consultation. The contents of the draft are then discussed at a meeting called "Fablab" in Brussels, together with representatives from data protection authorities, civil society and the business sector. A first draft of the guidelines is published (v1), subject to a second consultation of stakeholders that results in publishing a second draft (v2).[39]

Harmonising certification schemes

There are two simultaneous stakes here: specifying the rules of implementation of the GDPR, and regulating the European market for certification services. Indeed, the WP29

37 http://www.cencenelec.eu/standards/Sectors/DefenceSecurityPrivacy/Privacy/Pages/default.aspx

38 https://iconewsblog.wordpress.com/2015/08/28/whats-the-latest-on-the-ico-privacy-seals/

39 See the different adopted guidelines: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.

explains that "*experience in other areas such as in certification of goods has shown a tendency towards the bottom. Competition among service providers may lead to a reduction of prices and also to certain flexibility or relaxation of the procedures. [...] Rules seem necessary to ensure good quality of the services and a level playing field.*"[40] Doubts remain on how and to what extent European and national public authorities should intervene, given the large flexibility Member States have on implementation.[41]

In this respect, research has been carried out on how the experience of CE marking could be a useful case study in the context of the Internet of Things.[42] CE marking is based on the following scheme:[43]

- the EU legislator issues "high level" requirements through "new approach" directives;
- standardisation organisations issue the technical standards associated to these requirements;
- private manufacturers or certification bodies assess and certify compliance with these technical standards;
- Member States national authorities monitor manufacturers and certification bodies on their own market.

This co-regulation scheme implies that the European Commission adopt a mandatory standard regarding personal data protection to which organisations would self-certify. This would have the benefits of allowing for some flexibility, making it easier to involve small and medium-sized enterprises and reducing certification costs. However, there are two drawbacks to such an approach. First of all, CE marking is somewhat confusing for consumers, as it testifies that a product is presumed to comply with a European standard, not that it was made in the European Union, as some consumers seem to believe. Besides, this scheme is only applicable to goods so far. It would therefore need to be adapted to

40 Article 29 Data Protection Working Group, Opinion 3/2010 of 13 July 2010 on the principle of accountability (WP173), No 67, p. 18.

41 See Tambou, O., (2016). *L'introduction de la certification dans le règlement général de la protection des données personnelles : quelle valeur ajoutée ?, Revue Lamy de Droit de l'Immatériel*, April 2016, pp. 51-54.

42 See E. Lachaud on enlarging CE Marking to personal data protection, in Lachaud, E., (2016). Could the CE Marking Be Relevant to Enforce Privacy by Design in the Internet of Things? In Data Protection on the Move (pp. 135-162). Springer Netherlands.

43 Council Decision 93/465/EEC of 22 July 1993 concerning the modules for the various phases of the conformity assessment procedures and the rules for the affixing and use of the CE conformity marking, which are intended to be used in the technical harmonisation Directives, ECOJ, L 220, 30.8.1993, p. 23.

all services, individuals and procedures related to personal data. The fact that this possibility is mentioned nowhere in the GDPR seems to indicate the preference for a specific "Personal Data" seal.

Another possible scheme, not so far from CE marking, would imply adopting a mandatory standard on impact assessments.[44] Organisations would self-assess and self-certify. Verification would either be the responsibility of data protection authorities, or private certification bodies that would carry out annual or biannual third-party audits. Complaints could first be filed before the certified organisation, then sent before a court of law or a supervisory authority.

One solution could also be to establish seals at the national level. It would allow to keep both supervisory authorities and national markets onside, yet would entail coordination problems. The major risk would be that entities wishing to get certified turn to seals that are less demanding, easier to obtain and with a greater return on investment, since certification is "an ordinary market activity, fully open to competition."[45]

If the supervisory authorities are eventually put in charge of issuing certification, they will need to be afforded adequate human and financial resources to support this activity. Can this happen in the context of current budgetary restrictions? They will also have to make sure they avoid any form of discrimination or conflict of interests — such concern is often brought forward by stakeholders.

Words of a lawyer

"*A certification body cannot impose sanctions [...], as it would be tempted to favour those who have got the CNIL seal to the detriment of those who do not, yet might have [...] other seals, more demanding than the CNIL seal, without yet creating a presumption of conformity.*"

44 See Rodrigues, R., Wright, D. and Wadhwa, K. (2013). Developing a privacy seal scheme (that works), International Data Privacy Law Advance Access, published February 1, 2013, 17 pages,. p. 15.

45 Point 51 of Opinion of the French Competition Authority of 16 November 2015 reviewing standardisation and certification processes in the light of competition law, (*Avis de l'Autorité de la concurrence n° 15-A-16 du 16 novembre 2015 portant sur l'examen, au regard des règles de concurrence, des activités de normalisation et de certification, point 51*), http://www.autoritedelaconcurrence.fr/pdf/avis/15a16.pdf (FR)

For certification to be successful in a variety of situations, would it not be more efficient to allocate the resources of supervisory authorities to monitoring the level of independence and ability of experts working for private certification bodies? To be sure, there is a need to establish rules that pave the way for cooperation between supervisory authorities and national accreditation bodies, in order to monitor all certification schemes and coordinate the Personal Data seal with seals in other fields such as security.

The difficult issue of the level of protection still needs to be discussed. Should we think of certification as a facilitator that helps organisations demonstrate their compliance with specific quality criteria or as part of a global effort to raise the level of protection beyond what is specifically written in the legislation, like the seals issued by the CNIL? The risk would then be to micro- and over- regulate and fall short of stakeholders' expectations, especially small and medium-sized enterprises'.

There is still a long way to go before we see European "seals" that provide citizens with precise and credible information at a glance. Let's make sure we do not bring more confusion to an already complex field.

How to cite this chapter: Levallois-Barth C. "Certification mechanisms in the General Data Protection Regulation (GDPR)", *in Signs of trust – The impact of seals on personal data management*, Paris, Handbook 2 Chair Values and Policies of Personal Information, Coordinated by Claire Levallois-Barth, January, 2018, chapter 8, pages 135–151.
http://www.personal-information.org/

Chapter 9.

Economic analysis of personal data protection and privacy seals and marks

Patrick Waelbroeck
Antoine Dubus

9

We analyse in this chapter the economic issues raised by labels of personal data protection and by privacy seals. We first develop the notion of asymmetric information, which occurs when consumers are looking for signals to determine whether they can trust the products or services that they buy (9.1.). We continue with the analysis of the demand for privacy and for personal data protection (9.2.). We then answer the question of why do companies supply security and data protection (9.3.). We conclude this chapter by discussing the different economic models associated with the process of delivering labels and trust marks (9.4.).

9.1. Asymmetric information

The digital economy is “data-driven”. Internet companies such as Amazon or Criteo use personal data to develop their business models based on product recommendations and ad targeting.[1] This information can result from voluntary contributions (a consumer commenting on a blog or evaluating the quality of a product or the reputation of a seller) or involuntary traces (left by a user in his/her browsing history). This raises the question of what types of data companies use and what are the risks for consumers.

Data misuse can lead to negative externalities such as fraud, harassment, spam, hacking, identity theft, etc. These negative externalities result from a market failure when the

1 See https://www.criteo.com/ for a description of their business offers

Economic analysis of personal data protection and privacy seals and marks

actions of an economic agent have a negative effect on other agents without compensation linked to a market mechanism.

These risks are present at the stage of data collection, exploitation and transmission. Nevertheless, they are difficult to apprehend for the consumer. On the one hand, it is difficult for him/her to verify how his/her data are used by the companies that collect and process them and to know whether or not these treatment comply with the current legislation. This is especially true in the era of Big Data where independent databases with little personal information can be easily combined to identify a person. On the other hand, an individual is hardly able to technically assess the level of computer security during the transmission and storage of his/her personal data.

This situation leads to asymmetric information about the volume of personal data stored by the company and its partners, the effective treatment and the territories that host the data. Asymmetric information occurs when an economic agent has more information about the states of nature and the different types of uncertainties than another agent. This can lead to the disappearance of the market, as George Akerlof[2] has shown in his work for which he received his Nobel Prize.

2 Akerlof, G. A. (1970). The market for lemons: Quality uncertainty and the market mechanism. The quarterly journal of economics, 488-500.

The economic impact of asymmetric information was first analysed in second-hand markets, where a seller knows the quality of the product that he sells, better than the prospect, and then has been applied to the labour market and the financial markets. This concept can be applied to personal data because the company that processes the data of its customers has more information on the level of legal compliance and the level of security of its IT infrastructure than the user. However, companies themselves are not always able to fully assess the level of security of their information system: they sometimes do not know whether they have been cyber-attacked. In this case, the integrity of the data system is not verifiable and the status of security and protection may be unknown for both businesses and consumers. We speak of credence goods when the state of nature cannot be verified by any economic agent involved in the transaction.

Security of a transaction as a credence good

The case of Yahoo[3] illustrates this phenomenon on a large scale, since the firm only became aware (according to its say) in 2016 of the theft of more than one billion user accounts that had taken place three years before.

Asymmetric information can encourage unscrupulous sellers (i.e. those who do not comply with current regulations or good practices) to apply poor data protection policies and reduce the participation of consumers in the market. In the presence of asymmetric information, consumers seek signals to assess the level of privacy, of data protection, and/or of security of Web sites, products, and services. Among these signals, privacy seals and trust marks play a central role.

9.2. Demand for security and for personal data protection: analysing the sources of negative externalities

The main economic justification for protecting personal data is based on the existence of negative externalities for consumers when data circulate without authorization. These negative externalities can take the following forms:

3 http://www.lemonde.fr/pixels/article/2016/12/14/plus-d-un-milliard-de-comptes-d-utilisateurs-yahoo-ont-ete-pirates_5049069_4408996.html

- identity fraud and identity theft
- the use of personal data by a third party for questionable purposes such as spam
- the loss of personal data such as credit card numbers due to a lack of security of the servers where the data is stored

These negative externalities (for the consumer) lead companies to collect too much data compared to the social optimum. There are several other economic mechanisms that explain why consumers want to protect their personal data. We present them below.

Price discrimination

If companies have accurate information about their customers and their behaviour, they may practice price discrimination, i.e. selling the same product or service at different net prices to different consumers. The net price includes delivery and production costs. For digital products, the most common form of discrimination is to develop strategies in order to identify multiple consumer groups and offer different versions of the same product or service to these groups. For example, a software manufacturer offers the same product with different features: a full professional version and a basic (or student) version for which some features are not available. Personal information can therefore be used to customize offers to targeted customers, often at a very low cost. Some consumers benefit from low prices, but others are offered higher prices and may decide to protect their personal data to avoid being price-discriminated. Software that hide IP addresses and Internet browser extensions blocking scripts make it more difficult to identify users and therefore to price discriminate.

Targeting and filter bubbles

Consumers receive online information filtered by platforms such as Google or Amazon. For example, the Google search engine filters search results based on geolocation, browsing history, and ad profile. Amazon runs algorithms to provide product recommendations based on the user's browsing history and purchases. These information filters can influence the behaviour of Internet users. They raise important economic problems mainly related to competition law. Indeed, how can we guarantee that the consumer does not miss out on commercial opportunities and that these filters do not reduce competition by excluding some content, products or services?

Filter bubbles are generated by algorithms that create a specific universe for a user and can potentially influence the way the user thinks, behaves and buys. Again, some users may decide to protect their data against the algorithmic targeting.

Ads and ad blockers

Many online networks can be described by what the economic literature calls “two-sided markets”. They are characterized by cross-side or indirect network externalities between different groups of agents. For example, a search engine such as Google.com gives Internet users free access to content funded by advertising, connecting therefore advertisers with prospects. The value of the search engine to users increases with the number of relevant ads. Similarly, an advertiser looks for a platform with a large number of users who can see his targeted ads. There is therefore an indirect positive network externality between Internet users and advertisers. The dynamics of two-sided markets where Internet users and advertisers interact implies that a small initial comparative advantage of a search engine can lead to its dominance of the market through a positive feedback loop.

The economics literature on advertising distinguishes two types of advertising: informative and persuasive advertising. Informative ads provide information on key product characteristics, such as physical details, specifications, and prices. Persuasive ads are used to build a brand and do not necessarily provide useful information. Although informative advertising is valuable to some consumers, persuasive advertising can be considered a nuisance for others. The latter will then try to block them and avoid being identified.

Empirical work on consumer perceptions of advertising is rare, but highlights a variety of consumer attitudes: some adore advertising while others are extremely averse to it. These perceptions also vary from country to country. According to a study by Business Insider UK, one in four Internet users uses an ad blocker in France, while only one in ten uses it in the United States in 2015. The penetration rate of ad blockers is rising sharply in France and reaches more than 50% according to the survey conducted by the ***Chair Values and Policies of Personal Information*** in early 2017[4].

4 https://cvpip.wp.imt.fr/files/2017/06/Donn%C3%A9es-personnelles-et-confiance-VPIP-Mediametrie-Synth%C3%A8se.pdf [in french

ToS are difficult to read, … and to understand

Formal and written rules, such as terms of service (ToS) can reduce asymmetric information by specifying the level of computer security and legal compliance of the protection of personal data. ToS are often used by companies that sell digital products and services. However, as highlighted by Olurin et al. 2012[5], Anton et al. 2003[6], these ToS are extremely difficult to read and understand (Cranor and McDonald 2009[7], Becher and Zarksy 2015[8], Bakos et al., 2014[9]). In addition, they are always formulated in an "all or nothing" format where the buyer of the product or the user of the service must accept all conditions before they can use it. By analysing the economic impact of these contracts, we can think that the terms of services that better protect personal data will lead to a lower level of profitability in the short term. On the one hand, data protection and security are expensive to implement. On the other hand, the terms of service that facilitate the exploitation, reuse and sale of personal data generate more profits. A single contract for all users enables a company to impose flexible rules on the protection of personal data and is certainly not a guarantee for the user of the service that his/her personal data will be protected, thus creating and perpetuating asymmetric information.

9.3. The supply of security and of personal data protection by companies

We now study the factors that drive businesses to secure their data infrastructure and protect the personal data of their customers. First, security can be analysed as a public good for which there is underinvestment by the private sector. As we have seen in the previous sections, there are negative externalities associated with the lack of protection of personal data that are not compensated by market mechanisms and exacerbate this phenomenon of underinvestment. Second, companies are developing business strategies

5 Olurin, M., Adams, C., Logrippo, L. (2012). Platform for privacy preferences (p3p): Current status and future directions. IEEE, Tenth Annual International Conference on Privacy, Security and Trust (PST), pp 217-220. DOI : 10.1109/PST.2012.6297943

6 Anton, A., Earp, J. B., Bolchini, D., He, Q., Jensen, C., Stufflebeam, W. (2003). The lack of clarity in financial privacy policies and the need for standardization. IEEE Security & Privacy, 2(2):36-45. DOI : 10.1109/MSECP.2004.1281243

7 McDonald, A. M., Cranor, L. F. (2009). The cost of reading privacy policies. ISJLP, 4, 543.

8 Becher, S. I., Zarsky, T. (2015). Online Consumer Contracts: No One Reads, But Does Anyone Care?

9 Bakos, Y., Marotta-Wurgler, F., Trossen, D. R. (2014). Does anyone read the fine print? Consumer attention to standard-form contracts. The Journal of Legal Studies, 43(1), 1-35. DOI : 10.1086/674424

to quickly achieve critical mass sometimes at the expense of securing their data infrastructure. Finally, business strategies based on the exploitation of personal data often require companies to disclose their customers' personal data to third parties who do not necessarily receive incentives to protect them. Due to asymmetric information about the level of security of the data infrastructure, companies can easily share data without customers being aware of it.

Computer security as a public good

Economic theory characterizes a public good by a non-rival use, that is to say that the consumption of the good by an agent does not prevent another agent from consuming it. Public goods are also non excludable: it is difficult to prevent an agent from consuming the good. On the one hand, a company that secures its data infrastructure cannot usually take full advantage of its investment because other companies benefit from it.

It will therefore tend to underinvest in the security. If all companies follow this logic, there is a risk of underinvestment in security at the industry level.

In addition, companies have less incentives to secure their customers' data relative to the social optimum because they do not take into account negative externalities for digital users, as argued in the previous section. Overall, the private sector does not provide the optimal level of data protection and personal data can be weakly protected in the ecosystem.

The consequences of network externalities

Moore and Anderson (2012)[10] study the effect of network externalities on the level of security chosen by software developers. Positive externalities of networks arise when the value of a product or service increases with the number of users. For example, the value of a software increases with the number of its users, because it is easier to exchange files with friends, colleagues, and contacts in general. It is therefore important for a company to reach a critical mass as quickly as possible in order to dominate its market and become the best-selling product. The incentives for a company to spend money and time to protect the personal data of its customers are reduced, compared to a situation without network

10 Moore, T., Anderson, R. (2012). Internet security. The Oxford Handbook of the Digital Economy'(Oxford University Press 2011)

externalities. Letting computer security researchers, or independent professionals, correct bugs and then patch the software through updates, seems more cost-effective.

Business models based on data exchange

Companies that develop their business strategies around advertising generate revenue by selling their customers' data to third parties. These companies want to write very general terms of service so that they can fully use (and reuse) available data. When personal data is transferred to third parties, it is difficult for the customer to determine how his/her data is used, stored and secured. *Ad exchanges* with real-time bidding exacerbate these problems because the personal data available in the cookies stored on the computers are transmitted and matched by other platforms and third-party companies. Personal data can then be used without customer consent by companies that are sometimes remotely connected to the initial company.

Data lock-in

Economies of scale in the storage and treatment of data, the existence of network externalities on multi-sided online platforms, that is, serving as intermediaries between several groups of agents, have created monopolies on the Internet. For example, Google accounted for more than 88% of Internet searches worldwide in 2017[11]. In addition, a user of an online service benefits from information stored online that allows him/her to automate his/her connection, record his/her preferences and browsing history. This creates a lock-in situation resulting from captive users who are loyal to the service and characterized by high switching costs. This situation allows monopoly companies to impose terms of use of their services facilitating the massive exploitation of their customers' data sometimes at their expense (Mantelero, 2013[12]).

11 http://www.journaldunet.com/ebusiness/le-net/1087491-parts-de-marche-des-moteurs-de-recherche-dansle-monde/ [in french

12 Mantelero, A. (2013). Competitive value of data protection: the impact of data protection regulation on online behaviour, International Data Privacy Law 3(4): 229-238. DOI : 10.1093/idpl/ipt016

9.4. An economic analysis of labels of personal data protection and of privacy seals

Privacy seals can take different forms and have different features. We summarize the main ideas of the economics literature, referring to Rodrigues et al. (2013)[13] for a more systematic approach. A ***membership-based privacy seal*** is issued by an association to its members against fees. It is usually issued by a private company, such as TRUSTe in the United States. A ***public label***, for its part, is issued by a public authority in accordance with a regulation, a law or a specific policy. A ***binary privacy seal*** (public or private) indicates whether the company has achieved a certain level of certification of compliance with existing regulations or standards. A ***continuous privacy seal*** (public or private) has several levels of compliance, usually represented by letters or colours.

Membership-based label and public labels

An association delivering a label is less credible if its members join on a voluntarily basis, for obvious reasons. Indeed, the relationship between the organization that issues the label and its members is ambiguous. It is a "principal-multiple agent" relationship where members are also customers who pay a membership fee to the principal. The principal is interested in acquiring new members and therefore has less incentive to check the compliance of its members with the standards of the label even if the organization charter states that it is committed to doing so. As a result, members protect their customers' data only if they believe that the probability of being caught in default is high enough.

Public labels do not suffer from the problem of clientelism, but the question of financing the audit process arises, as we will see later on. In addition, public labels often co-exist with private membership-based labels. How do you determine the reference level of the public label? First, a label provided by a government body that is too weak compared to industry best practices loses its signalling power. Some companies will then prefer to pay an additional cost to adopt a high quality private label in order to attract customers and gain a competitive advantage as well as a better reputation.

13 Rodrigues, R., Barnard-Wills, D., Wright, D., De Hert, P., Papakonstantinou, E. (2013). EU Privacy seals project: Inventory and analysis of privacy certification schemes. Final Report. Publications Office of the European Union.

If the public norms are close to those of the industry best practices, companies will rely on the public label to display the high quality of their personal data protection policy; the public label then replaces the private label. Finally, if there are only public privacy seals, there is a risk of adverse selection that can lead to the exclusion of high quality companies if the public standard is too low (or medium to high quality companies if the standard is too high).

Finally, the coexistence of international privacy seals, subject to different legislations, can de facto create a cohabitation of public and private labels in the data protection ecosystems. ***Determining the reference level for the standard of protection is therefore an essential element to consider when designing a label of data protection.***

Formats: voluntary, continuous, binary

Two main formats of labels exist, which have different economic effects: continuous and binary. Continuous labels take different values, represented by colours, signs, or letters. A binary label only indicates whether the company reaches a referential point. Roe and Sheldon (2007)[14] find that continuous labels significantly reduce asymmetric information and lead to market prices and quality equivalent to those prevailing in a perfect information situation, even though continuous labels are a priori more difficult to understand and interpret than binary labels. For binary labels, there is a risk that low-income consumers and low-quality companies may prefer the lower quality standard, and high-income consumers may prefer companies with a high level of protection.

Audit procedures and conflict resolution

Sometimes, the contract between the organization that issues the label and its members specifies that members pay to resolve conflicts with customers. Sometimes customers have to pay the litigation costs. This can lead to inefficiencies if the fees are high. For example, Connolly (2008)[15] demonstrated that the application of the terms of the contract between TRUSTe and its members was rare. He provides many examples of privacy breaches between 1998 and 2007 (including data breaches at AOL, Facebook, Hotmail, Microsoft and Real Networks) that were not followed by corrective actions.

---

14 Roe, B., Sheldon, I. (2007). Credence good labelling: The efficiency and distributional implications of several policy approaches. American Journal of Agricultural Economics 89(4):1020-1033. DOI : 10.1111/j.1467-8276.2007.01024.x

15 Connolly, C. (2008). Trustmark Schemes Struggle to Protect Privacy, Working paper.

It is obvious that a private label without a regular audit policy is set to lose its quality signalling power to consumers.

Business models

The next question is related to fees charged by the organization that delivers the label. On the one hand, a high price for a label excludes small businesses that cannot afford the labelling process. On the other hand, a high price signals to consumers that the company displaying the label is financially sound and has sufficient resources to protect the personal data of its clients.

A high price also reflects the good reputation of the organization that delivers the label and the reliability of the labelling process. This argument is obviously valid only if Internet users know the costs of labelling paid by the companies that manage the websites that they visit.

A low price does not allow the label to play its role as a signal of quality and could reduce the budget of the organization delivering the label to audit its members. A free certification is only possible if it is financed by a consortium or a public agency. The question of the cost associated with public labels is still open.

Several economic factors highlight inefficiencies in the market for personal data protection. First, asymmetric information creates opportunistic behaviour from unscrupulous companies who develop strategies to exploit customers' data, sometimes without their knowledge (price discrimination, ToS offering too little protection, captive customers). Secondly, companies that invest in customer data protection often do not take into account negative externalities due to data breaches (spam, identity theft, fraud). Third, market forces are pushing some companies to reach a critical mass at the expense of data protection. Other companies base their business model on the sale of data to third parties who do not necessarily have the same economic incentives to protect customer data. Data protection labels act as a signal of trustworthiness, but the economic impact of these labels is difficult to determine. On the one hand, a high-quality label delivered by a public institution generates trust but is costly both for private companies that need to spend resources to comply with the standard and for the public institution that needs to finance the process of auditing.

On the other hand, a private label solves the problem of financing the audits, but poses problems of clientelism and can be manipulated. In both cases, the questions of knowing what is the reference level of the standard associated with the label and its price are essential for the label to fully play its role of a signal of economic trustworthiness.

How to cite this chapter: Waelbroeck P., Dubus A. “Economic analysis of personal data protection and privacy seals and marks”, *in Signs of trust – The impact of seals on personal data management*, Paris, Handbook 2 Chair Values and Policies of Personal Information, Coordinated by Claire Levallois-Barth, January, 2018, chapter 9, pages 153–165.
http://www.personal-information.org/

« En Chemin l'empreinte de l'autre » – Thierry Citron

Chapter 10. The economic impacts of labels

Patrick Waelbroeck

10

This chapter looks at the economic impact of labels for businesses and consumers. In this chapter we use the words label, seals and (trust)marks interchangeably. The word "label" is used in many industries such as in the agricultural sector. The GDPR prefers the terminology "data protection and privacy seals or marks". We first show how labels and trust marks can impact business strategies (10.1.). The results presented are mainly based on American studies which can nevertheless be used in the European context. Section 10.2 presents the results of a survey conducted by the ***Chair Values and Policies of Personal Information*** in 2017 in collaboration with Médiamétrie on the use of personal data by French Internet users.[1] The section on how labels are perceived by Internet users is presented exclusively in this chapter.

10.1. Economic impact of labels and trust marks on business strategies

Empirical studies of the economic effectiveness of trust marks and labels show that they lead to a small increase in retail prices and that they increase sales. These studies also identify that the behaviours adopted by consumers may present some risks because they sometimes misunderstand personal data protection and privacy policies. To give an

1 https://cvpip.wp.imt.fr/donnees-personnelles-et-confiance-quelles-strategies-pour-les-citoyens-consommateurs-en-2017/

The economic impacts of labels

order of magnitude, we can refer to the study by Miyazaki and Krishnamurthy (2002)[2] who found that in the United States 32% of Fortune 50 companies, nearly 5% of Fortune 500 companies and 14% of Information Week 100 companies were showing a TRUSTe or BBBOnLine seal, the two major US seals in 2002. More recent studies show similar figures for the adoption of privacy seals and trust marks among the TOP 50 most visited websites (about 7 out of 50).

Increase in price and sales

The various American studies show that, after the adoption of a label, the price of the labelled product increases. The impact varies according to exogenous factors. Different orders of magnitude make it possible to disentangle these impacts according to the nature of the product, the type of label, the process or component being labelled, or the geographical location of the market. Since the literature focuses on agricultural labels, the effects need to be interpreted with caution, but they make it possible to grasp the main economic effects.

Kiesel and Villas Boas (2007)[3] study the impact of the National Organic Program and of the US Department of Agriculture organic milk labels on consumers in the United States.

2 Miyazaki, A. D., Krishnamurthy, S. (2002). Internet seals of approval: Effects on online privacy policies and consumer perceptions. The Journal of Consumer Affairs 28-49. DOI : 10.1111/j.1745-6606.2002.tb00419.x

3 Kiesel, K., Villas-Boas, S. B. (2007). Got organic milk? consumer valuations of milk labels after the implementation of the USDA organic seal. Journal of agricultural & food industrial organization 5(1). DOI : 10.2202/1542-0485.1152

They find a change in the buying habits of consumers after the creation of the labels. Specifically, a price mark-up of between 192 cents and 224 cents is accepted by consumers for half a gallon of organic milk, which corresponds to an increase of 39.4% to 45.8% of the retail price.

Brounen and Kok (2011)[4] studied the evolution of Real Estate purchases in the presence of an energy label in the Netherlands. They observed an increase of 3.7% in the propensity to pay, linked to the presence of a label guaranteeing a higher energy efficiency of the home. Considering that the average selling price of a home in the Netherlands during their study was 231 000 €, they estimate the average price increase to 8 449 € due to the existence of the label.

In the case of agricultural labels, McCluskey and Loureiro (2000)[5] refer to a 1997 study in France (after the mad cow crisis). They report a higher willingness to pay of 22% for non-infected guaranteed beef. Bjorner et al. (2004)[6] study the impact of the ecological label "Nordic Swann" on the consumption of 1,596 Danish households. The environmental label has a positive effect on the choice of toilet paper, with an increased propensity to pay of 13% to 18% for a product that is environmentally friendly.

From a commercial point of view, Levy et al. (1985)[7] observe a positive impact of the Special Diet Alert, a two-year nutrition information program launched by supermarkets. However, they note a difference in the impact of the program depending on the geographical area: the increase in product sales induced by the program was 4 to 8% higher in Washington than in Baltimore, putting forward a greater sensitivity of the population under study to the features of the labels.

---

4 Brounen, D., Kok, N. (2011). On the economics of energy labels in the housing market. Journal of Environmental Economics and Management 62(2):166-179. DOI : 10.1016/j.jeem.2010.11.006

5 Loureiro, M. L., McCluskey, J. J. (2000). Consumer preferences and willingness to pay for food labelling: A discussion of empirical studies. Journal of Food Distribution Research 34(3):95-102

6 Bjørner, T. B., Hansen, L. G., & Russell, C. S. (2004). Environmental labelling and consumers' choice—an empirical analysis of the effect of the Nordic Swan. Journal of Environmental Economics and Management, 47(3), 411-434. DOI : 10.1016/j.jeem.2003.06.002

7 Levy, A. S., Mathews, O., Stephenson, M., Tenney, J. E., &Schucker, R. E. (1985). The impact of a nutrition information program on food purchases. Journal of Public Policy & Marketing, 1-13

Mai et al. (2015)[8] study the impact of personal data protection labels on retail prices. They estimate a 1.5% price increase associated with the introduction of a data protection label by e-commerce websites. Similarly, Melnik and Alm (2002)[9] find a significant impact of a good eBay seller rating on sales, but a very small effect on prices.

The estimates we have just quoted therefore vary from 1.5% to 45.8% of the retail price of a product signalled by a label, compared to a product that does not show any label. The list of studies above shows that the location of the sale, the nature of the product, and the existence of possible scandals related to the sector studied are probably the cause of such differences. This result can be summarized by the intuitive notion of perceived risk. A user will be ready to pay a higher price increase for a product if the risk associated with a questionable product quality is important.

More specifically, McCluskey and Loureiro (2000)[10] show that non-GMO labels in Europe and in Japan increase the willingness to pay of consumers, while Li et al.(2003)[11] find in China that consumers are willing to pay 38% more for genetically modified rice compared to traditional rice, and 16.3% more for genetically modified soybean oil compared to traditional soybean oil. This could be explained by differences in cultures and agricultural policies.

Labels have a greater effect on volume than on price, especially for websites sites that do not charge a price for its service (the majority of Internet companies do not charge any price to their users), since the impact of a label cannot have a price effect in this case.

8 Mai B, Menon N M, Sarkar S (2010) No free lunch: Price premium for privacy seal-bearing vendors. Journal of Management Information Systems 27(2):189-212

9 Melnik, M. I., &Alm, J. (2002). Does a seller's ecommerce reputation matter? Evidence from eBay auctions. The journal of industrial economics, 50(3), 337-349. DOI : 10.1111/1467-6451.00180

10 Loureiro M L, McCluskey J J (2000) Consumer preferences and willingness to pay for food labeling: A discussion of empirical studies. Journal of Food Distribution Research 34(3):95-102

11 Li, Q., Curtis, K. R., McCluskey, J. J., & Wahl, T. I. (2003). Consumer attitudes toward genetically modified foods in Beijing, China

Too many labels create confusion

Gao (2007)[12] compare the impacts of different label features. He lists four characteristics of an agricultural product that can be guaranteed by a label: consumer quality measured in terms of tastefulness, geographical origin, organic production methods, presence of GMOs.

The originality of his approach lies in the comparative study of the existing labels, and the study of the additional impact of a label on a product that is already labelled. They note, among other things, that the expiration date has a second-order impact, depending on the presence of other attributes. In addition, the labels on the tenderness and low fat of the meat have a significant positive effect, contrary to the expiration date. Surprisingly, the marginal effect of the origin of the product change after a threshold. Adding a fourth label increases the willingness to pay, adding a fifth label decreases it.

The important thing to notice here is the change in the effect from a positive value to a negative value, suggesting that the number of labels can be judged negatively after some threshold. Finally, he observes that, without taking into account the precise nature of the labels, their number has a positive marginal effect.

This confusion effect is also pointed out for ecological labels by Leire and Thidell (2005).[13] They study the impact of the "Nordic Swann" label and find that this label is effective in the following way. Consider two similar products. Consumers declare that they have a stronger purchase intention for the product that displays the "Nordic Swann" label. However, this result becomes weaker when the author considers the actual purchase.

Finally, if we consider personal data on the Internet, Larose and Riffon (2007)[14] analyse the behaviour of 227 students and conclude that the "*Privacy Paradox*", i.e. the voluntary

12 Gao, Z. (2007). Effects of additional quality attributes on consumer willingness-to-pay for food labels (Doctoral dissertation, Kansas State University)

13 Leire, C., Thidell, Å. (2005). Product-related environmental information to guide consumer purchases–a review and analysis of research on perceptions, understanding and use among Nordic consumers. Journal of Cleaner Production, 13(10), 1061-1070. DOI : 10.1016/j.jclepro.2004.12.004

14 LaRose, R., Rifon, N. J. (2007). Promoting i-safety: effects of privacy warnings and privacy seals on risk assessment and online privacy behavior. Journal of Consumer Affairs, 41(1), 127-149. DOI : 10.1111/j.1745-6606.2006.00071.x

sharing of personal data despite the fear that they are not actually protected, is due to too much user trust that can lead to a certain vulnerability of the users.

However, Nouassair et al. (2002)[15] study a phenomenon comparable to the "*Privacy Paradox*", in the context of genetically modified products in France. Consumers surveyed declare that they are against genetically modified foods. However, they do not seem to take this component into account when shopping. Their study of a panel of 112 participants underlines that the inattention to labels is the cause of this contradiction, and that the price they are willing to pay decreases by 30% when consumers become aware of the presence of GMOs.

10.2. **Impact of labels on users**

In order to better understand how French Internet users manage their personal data, the ***Chair Values and Policies of Personal Information*** joined forces with Médiamétrie to conduct a survey in March 2017. This time period corresponds to a slow erosion of trust on the Internet, the often abusive collection of personal data and the surveillance put in place by some governments or private actors.

The sample, representative of the French Internet population, consisted of 2051 Internet users aged 15 and over. The representativeness was ensured by the quota method based on gender, age group (5 groups), socio-professional category (5 categories) and region (Paris region/other regions), established by matching quotas from the authoritative survey of the Web user population in France: *Observatoire des Usages Internet*. The questionnaire was self-administered online from February 26 to March 16, 2017.

To better understand the issues at stake, the series of questions written by Patrick Waelbroeck, Armen Khatchatourov and Claire Levallois-Barth focused on ***the forms that a label should take, on which actor should deliver the label, and on the impact of a label on the habits of Internet users***.

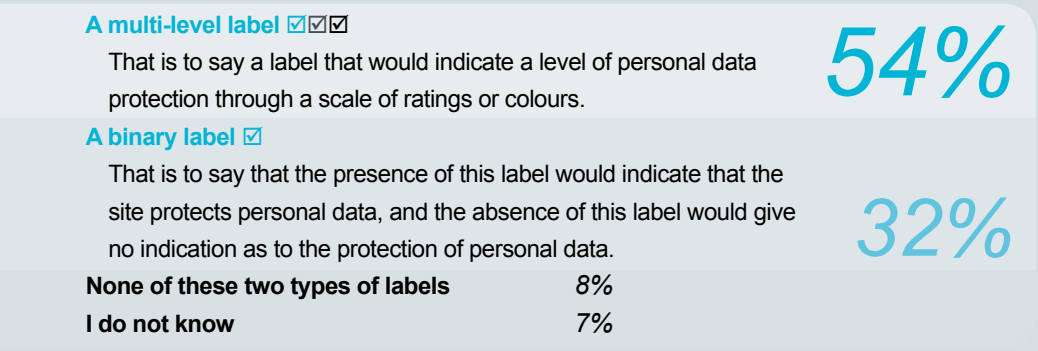
15 Noussair, C., Robin, S., Ruffieux, B. (2002). Do consumers not care about biotech foods or do they just not read the labels? Economics letters, 75(1), 47-53. DOI : 10.1016/S0165-1765(01)00594-8

Types of labels

We discussed the pros and cons of different forms of labels, in particular multi-level labels and binary labels (see Chapter 9). We have also underlined the risks of manipulation by labelled companies in the presence of binary labels. We concluded that a multi-level label was preferable. The answers provided by the Internet users that we surveyed confirm the preference for multi-level labels..

Figure 4. *Type of label and trust*

Of the internet users who say they prefer the presence or not of a data protection label, more than half would trust a multi-level label, which would express the level of personal data protection through a scale (of ratings or colours).



► *Question: which type of label would you trust most?*

► *Base: Internet users aged 15 and over who find a data protection label useful (n=1437)*

Who should label?

We identified in chapters 7 and 9 the risks of clientelism and the potentially perverse effects of a label issued by a private organization.

The predominance of the public body

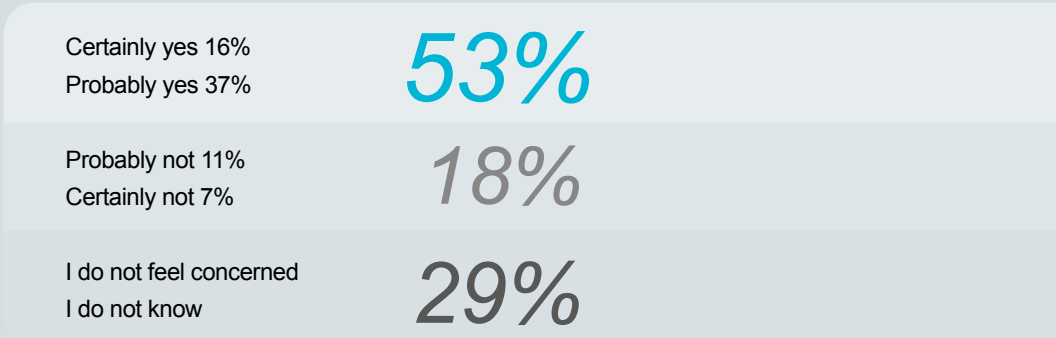
The responses to the survey clearly show that a government agency or an institutional body would be a trusted third party for almost 7 out of 10 Internet users. The question of the business model and the financing of the cost of the label was not asked.

The potential of a collaborative rating system

We find that 53% of respondents are ready to participate actively (without monetary or other incentives) to the collaborative rating system, which corresponds to a figure found for the eBay rating system, where about 50% of the members rate their transactions.

Figure 5. Willingness to contribute to collaborative rating system on the trustworthiness of a website

More than half of Internet users would be ready to give their opinion on the trustworthiness of a website to tell whether or not that the website protects personal data. On the other hand, 3 out of 10 Internet users do not feel concerned or do not know.



► *Question: To demonstrate that they protect personal information, some sites post consumer opinions on their trustworthiness. Would you be willing to participate by giving your opinion on the trustworthiness of a site?*

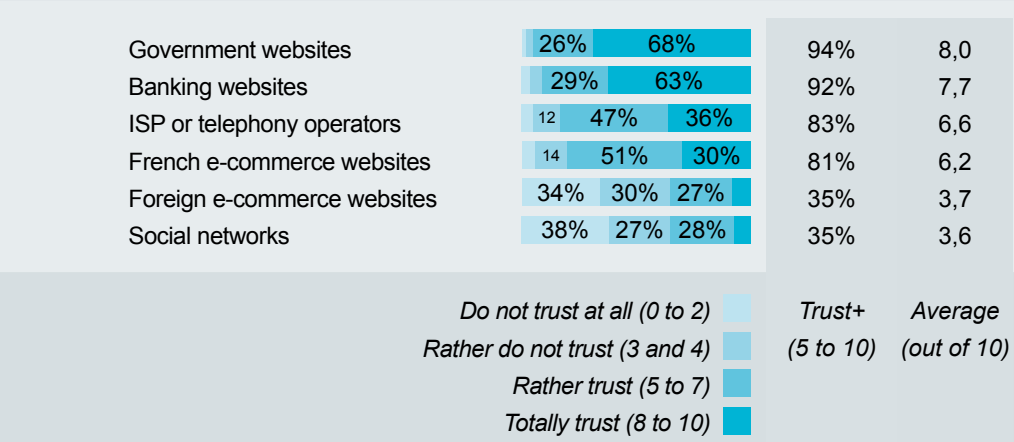
► *Base: Internet users 15 years and older (n = 2051)*

Who should be labelled?

The survey clearly shows that foreign online e-commerce websites and social networks, whose trustworthiness levels are well below average, must be labelled as a priority.

Figure 6. Level of trust vis-à-vis the actors on the Internet

Government and banking websites are trusted by almost all Internet users. French e-commerce websites are considered significantly more trustworthy than foreign e-commerce websites. Only a third of Internet users trust social networks (average score of 3.6 / 10)



► *Question: on a scale of 0 to 10, rate the trustworthiness of each of the following actors?*

► *Base: Internet users 15 years and older (n = 2051))*

Impact

The data protection label improves the level of trust in situations perceived as risky, for instance when using of a free service or when downloading a file from an unknown source. Internet users would also be ready to explore unfamiliar websites, which would allow them to get out of their filter bubbles. An economic impact for one out four respondents is also noteworthy.

Figure 7. Impacts of a data protection label

Among those who expressed a preference for the presence or absence of a label, more than three quarters consider that their browsing habits would be influenced by the presence of a label. This would notably improve the trust towards the labelled sites.

► *Question: if a personal data protection label was developed, would you…*

► *Base: Internet users aged 15 and over who are in favour of the label concept (n = 1437)*

Guidelines

Studies on the impact of labels in other industries, such as the agricultural or the energy sector, show that labels can have significant impacts in terms of price and sales for labelled products. The magnitude of these economic effects, however, varies from case to case, with the strongest effects being observed when the risks to consumers are high (health risks, for example).

Thus, the increasing awareness of Internet users about the societal issues around the protection of personal data lead us to believe that the economic impact of data protection labels will increase as well.

Turning to the perception of Internet users of such a label, the survey that ***Chair Values and Policies of Personal Information*** conducted in 2017 seems to indicate that a multi-level label issued by a public body combined with a collaborative rating system in co-construction with Internet users looks promising. It should primarily target foreign e-commerce websites and social networks.

How to cite this chapter: Waelbroeck P. “The economic impacts of labels”, *in Signs of trust – The impact of seals on personal data management*, Paris, Handbook 2 Chair Values and Policies of Personal Information, Coordinated by Claire Levallois-Barth, January, 2018, chapter 10, pages 167–178.

http://www.personal-information.org/

Chapter 11. Is blockchain a trustworthy technology?

Maryline Laurent

11

This chapter relies on a specific example of technology, the blockchain, to explain how the concept of "trust by design" presented in Chapter 1 can be implemented and what its limits are.

Blockchain technology was developed towards the end of the 2000s, within a wider project related to the transfer of cryptocurrencies over the Internet: Bitcoin. This project made blockchain technology popular and demonstrated its reliability. In 2014, the not-for-profit Ethereum headed by Vitalik Buterin began working on the idea that this technology should be extended to include some code to enable a new type of transaction: "smart contracts."

► Examples of smart contracts include launching a cryptocurrency transfer once a parcel is delivered or prepaying for a rental service in order to open a door (e.g. of a vehicle or a house).

In 2015, a first version of the source code of Ethereum was made public, allowing many industrial players and independent developers to innovate and offer services on top of this technology. Recently, Axa issued Fizzy, which offers compensation to passengers whose flights are delayed.[1]

1 https://www.coindesk.com/axa-using-ethereums-blockchain-new-flight-insurance-product

Is blockchain a trustworthy technology?

Blockchain is often compared to a large, publicly accessible and auditable ledger managed by its "members." Members can add entries to the ledger after obtaining approval from several other members, or in some cases the majority. It is therefore possible to track the entries added by each member, without necessarily knowing who wrote the entries since members use pseudonyms.[2]

After introducing the fundamental building blocks that help understand blockchain (11.1), we describe how this technology works at a technical level (11.2.). We then identify the key features that introduce a level of trust (11.3.). Finally, we draw up an overview of the risks and limits associated with this technology and discuss its ability to guarantee personal data protection (11.4. and 11.5.).

A major difficulty is to tease out the features strictly associated with the concept of blockchain and the ones associated with its different implementations, e.g. Bitcoin, Ethereum, Ripple, or Litecoin.[3] The explanations we give in this article are mostly related to Bitcoin, which is more consistently studied in the literature.

2 A member is pseudonymous when they are using an alias instead of their actual identity.

3 We will refer to these specific implementations as Bitcoin blockchain, Ethereum blockchain, and so on.

11.1. The fundamental building blocks

The security that blockchain offers mostly relies on standard cryptographic mechanisms, notably public key cryptography, hash functions and digital signatures.

Cryptographic mechanisms

Public key cryptography implies that every entity in a system has two keys: a public key shared with everyone, and a private key known only to the owner. The ***private key*** is a binary string enabling owners to prove their identities, e.g. sign a transaction request to prove they initiated it. The public key allows other entities to authenticate this signature.

The security level of a cryptosystem can be measured by how hard it is to find its private keys. This level is directly proportional to the size of the parameters: the larger they are, the harder it is to find the private key. However, as computers become cheaper and their processing power and memory bigger, the size of these parameters needs to increase on a regular basis in order to maintain the same security level. This level is measured by how many operations the attacker needs to make in order to crack the cryptosystem. Nowadays, a security level of 100 is considered sufficient — meaning attackers would need to perform 2^{100} operations to break the system.

The Bitcoin project relies on Elliptic Curve Cryptography (ECC) and the Elliptic Curve Digital Signature Algorithm (ECDSA). ECDSA uses elliptic curves to provide keys that are reasonably sized compared to other public key infrastructures such as RSA for the same level of security. For instance, in RSA (named after its inventors, Rivest, Shamir and Adleman), for a security level of 112 (2^{112} operations), the RSA key length is 3072 bits (i.e. a string of 3072 zeros and ones) while the ECC key length is only 256 bits.

Hash functions

Hash functions are very important in blockchains, especially SHA256. They allow to use private keys to craft signatures and authenticate transactions, reliably link a blockchain member to their public key, and therefore identify the source of a transaction or a block into the blockchain. They are also used to create chained links between the blocks so that their order cannot be modified, therefore offering some form of guarantee of the blockchain's integrity.

What are the properties of cryptographic hash functions

- They give a fixed-size result (or a *hash*): regardless of the entry, the function always returns a result of the same size. For instance, SHA256 always returns a fixed 256-bit hash.
- One-way function: it is very difficult[4] to find the entry based only on the function's result;
- Collision resistance: it is very difficult to obtain the same result for two different entries;
- Avalanche effect: changing one bit in the entry entails a change in more than half of the result's bits. This property is crucial in guaranteeing the integrity of entries since any modification is easily detected.

Digital signatures

The signing process begins with the application of a hash function to the elements of the transaction that third parties want to authenticate. Then, the signing party encrypts the result with their private key.

11.2. How blockchains work

A blockchain is a set of individual transactions grouped into blocks, where each block contains the transactions emitted since the last block was added to the blockchain. Each transaction is emitted by a member node that has already been enrolled, which then broadcasts it to all the members of the blockchain.

The authenticity[5] and legitimacy[6] of the transaction are then verified by the other nodes of the blockchain, which rely on the history of transactions recorded since the beginning of the blockchain. Then, miners combine all approved transactions into a batch that they add to the block they are building. They validate the block by mining, i.e. solving a complex math-

4 In the context of this document and of cryptography in general, "very difficult" suggests that current algorithms and computing resources cannot allow for an attack on a hash function in a reasonable time frame (several billiard years on one computer).

5 An *authentic* transaction is a transaction for which the emitting node has been authenticated.

6 A *legitimate* transaction is a transaction that the emitting node is authorised to initiate (i.e. the node has sufficient funds).

ematical puzzle called Proof of Work (PoW).[7] The first miner to solve the mathematical puzzle broadcasts the solution to all the nodes, which check the PoW. Once the solution is approved and the block has been added to the blockchain, miners begin to mine for the next block. As many nodes contribute to writing the block into the blockchain, this process relies on a consensus among nodes — this consensus principle becomes an essential characteristic of the governance structure of the blockchain.

Different types of nodes

From a technical perspective, members of the blockchain are computing resources (i.e. computers) that are connected to the blockchain through an *enrolment* phase. They belong to a network connected through the Internet and are usually called *nodes*.

To become a member of a blockchain, a person therefore needs to enrol a computer resource as a node. There are two types of nodes::

- ***regular nodes***, which for the most part have regular computing power, from which transaction requests can be emitted;
- ***miner nodes***, with large computing power that is useful to the blockchain, also able to submit transactions.

Both types of nodes can store the whole blockchain, provided they have enough memory. They are then called *full nodes*. The Bitcoin blockchain, launched in 2009, was more than 190GB in 2018.

The enrolment phase

During enrolment, nodes, both regular and miner, download a software that enables them to interface with the blockchain. This software is tailored to a personal blockchain account number (i.e. a 160-bit Bitcoin address) and a set of public and private keys. The node owner is required to keep the software and password to access their private key. If they lose one or the other, access to the blockchain account will be lost and no transaction may ever be emitted from that account again.

The link between the account number and the public key needs to be obvious and easy to check in order to authenticate the origin of a transaction request. In the case of the

7 The Proof of Stake scheme is fundamentally different from the Proof of Work, as explained page 190.

Bitcoin, the address is simply the result of the hash function on the public key, so that any node can authenticate the owner of an account as the entity behind a transaction. This bypasses the need for a key management infrastructure, which is interesting because managing electronic certificates[8] is both burdensome and costly.

The transaction phase

In the transaction phase, all transactions are validated, combined into a block, then mined (through PoW or PoS) — which typically takes several minutes (around 10 minutes for the Bitcoin project). The new block is then broadcast and added to the blockchain, after checking that the mining was successful.

Each blockchain gives the initiating node a certain degree of freedom regarding the conditions that need to be met for the transaction to be legitimate and authentic.

For Bitcoin, the implicit legitimacy condition is that a node should possess more Bitcoins than it is trying to transfer. The initiating node may also add a script requirement for authentication conditions: for instance, that the beneficiary node prove its identity by sending a valid digital signature, or multiple ones in case the owner owns multiple accounts and wishes to augment the level of security.

For Ethereum, the conditions are set by Smart Contract authors.

Regardless of the specific conditions adopted by each blockchain, a transaction always needs to contain (see Figure 8):

- a unique transaction identifier.
- information enabling to verify the transaction and to the least establish its context. In the bitcoin blockchain, it is required to provide inputs to a transaction that enable the initiating node (Bertrand) to identify anterior transactions (Anne's and Alice's) and check the legitimacy and authenticity of the current one: whether Bertrand has the necessary Bitcoin resources as well as the cryptographic conditions that are required by Anne and Alice (i.e. a public key and a digital signature) to prove he is the recipient of their money transfer.

8 An electronic certificate is a data structure that links a public key with its owner's ID in a secure way.

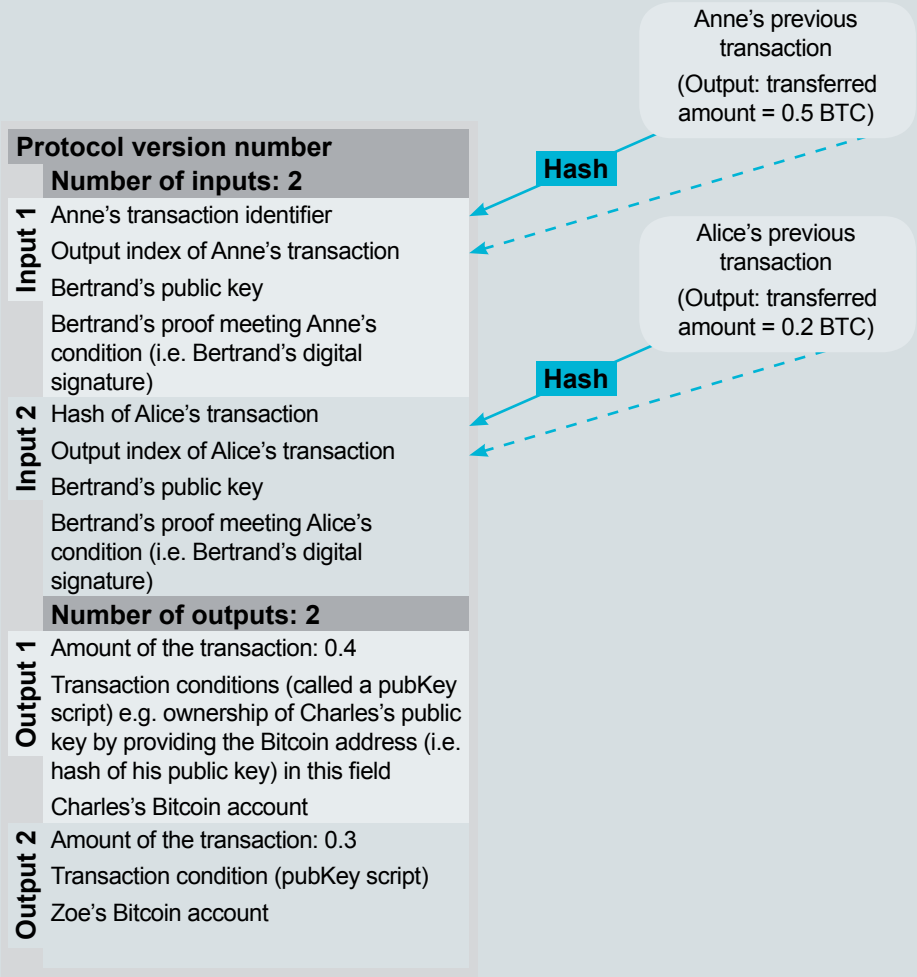


Figure 8. Simplified structure of a Bitcoin transaction

- information on the transaction result. Bitcoin also specifies outputs such as the transaction's recipients (Charles and Zoe), the amount, and the conditions that recipients need to meet to claim this sum. As in any ledger, inputs and outputs can have equal amounts, and if an output is lower than the sum of the inputs, then the miner receives the difference to compensate for the mining work. Such transaction fees are sometimes necessary to incentivise miners to prioritise transactions offering higher compensations in the block they are mining, leading to miners competing for the highest-paying transactions on the blockchain.

Creating the blocks

A block is made up of a batch of transactions, which it writes into a block so that their content as well as the position of the block within the blockchain cannot be altered in the future, be it through an accident or an attack. This protection against accidents and attacks relies on two necessary complementary processes.

The first process provides the series of transactions and blocks with a chained structure by linking them into a chain. This process relies heavily on hash functions and on the principle of a Merkle tree.[9] Hash functions prevent the partial modification of a block within the blockchain, which would trigger the avalanche effect, but they cannot protect against overwriting the last blocks, as we explain in section 11.3. For these blocks, the mechanism of mining together with a decentralised storage and computing architecture offers a level of trust. The elements providing a structural as well as a functional measure of trust are presented in 11.3.

As regards the specific Bitcoin structure (see Figure 9), a block contains a header including technical information on the blockchain, content including transactions, and a nonce, which is a random number used for mining, as well as other elements we explain below.

During each transaction, an identifier is computed (TxID), equal to the hash of the transaction's content. The Merkle tree then enables to securely add this transaction to the chain by calculating the hashes of all the blocks up to the root of the tree. The result of these

9 "*A Merkle tree is a tree in which every leaf node is labelled with the hash of a data block and every non-leaf node is labelled with the cryptographic hash of the labels of its child nodes. [Merkle] trees allow efficient and secure verification of the contents of large data structures.*" Wikipedia: https://en.wikipedia.org/wiki/Merkle_tree

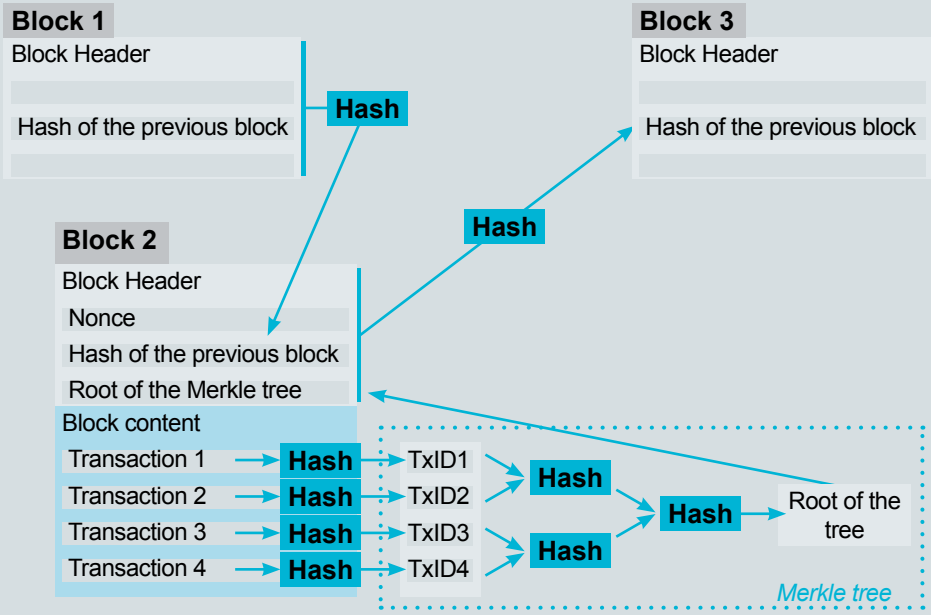


Figure 9. Simplified format of a Bitcoin block and its chaining to the blockchain

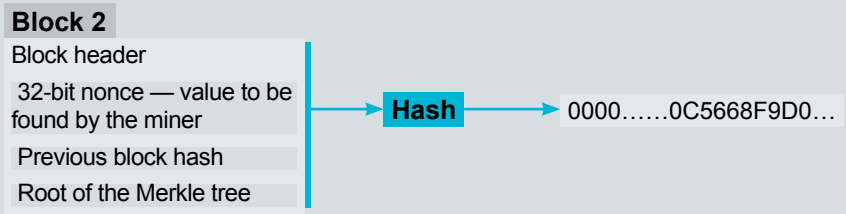


Figure 10. PoW mining on Bitcoin header

calculations is then written in the block's header, which is one way to check the block's integrity later on.[10]

The second process guarantees the integrity of the block's place within the blockchain by chaining the blocks into a series starting with the "Genesis Block."

► In Figure 9, block 2 is chained between blocks 1 and 3. Its location can be verified by checking that block 1's hash corresponds to the hash in block 2's header, and similarly block 2's hash in block 3's header.

When the PoW puzzle is solved by two (or more) miners simultaneously, the other nodes receive two different validated blocks. These are both added to the chain at the same level, which in practice creates a fork and two different blockchains.

This forking problem is self-regulated, because the mining effort is unequally distributed between the two temporarily distinct blockchains. The blockchain relying on the largest amount of computing power will grow faster and thus be recognised as valid — this is a first security vulnerability, as we explain in more detail in 11.3. For the Bitcoin blockchain, once 100 blocks have been added, forking problems are supposed to be solved. This obviously implies adding the transactions of the abandoned blockchain that are not in the validated blockchain back into it. Another convention is that a Bitcoin transaction is only considered effective once it's been buried under 6 blocks, which requires an hour wait before the recipient can use the Bitcoins it has received for another transaction. This condition is one of the main issues of blockchains in dynamic environment, which has led researchers to consider alternatives such as Proof of Stake (see 11.2).

How mining operations are confirmed

Mining enables miners to build a valid block by solving a complex mathematical puzzle and earning compensation for it. Before solving the puzzle, the miner adds a transaction named "coinbase" in the block for this compensation. The blockchain policy consists in enabling the miner to create some amount of currency and to ignore the rule for standard

10 To check the integrity of a block, the verifier has to successively perform the exact same Merkle tree hashing operations to locally compute the Root of the Merkle tree, then has to check that the result matches the value given in the field "Root of the Merkle Tree" of the block header. In case it does not match, the block is detected as corrupted.

transactions according to which the output needs to be lower than the input. The miner thus uses the "coinbase" transaction to specify the recipient and amount of the reward. This way, after the puzzle is solved and if the block is accepted by the other miners, this amount and the transaction fees are transferred to the miner who solved the puzzle. For Bitcoin, the reward per block decreases over time, and miners increasingly rely on transaction fees for their compensation.

Validation by Proof of Work (PoW)

To validate a block, miners have to solve a puzzle, i.e. to find a 32-bit nonce to add to the block's header so that the header's hash is lower than a threshold value called *difficulty* (see Figure 10). The lower this threshold, the harder the problem. The blockchain policy is to adjust the difficulty so that the difficulty (interpreted as a level of security) remains constant.

- For Bitcoin, a block is validated every 10 minutes, on average. After 2016 blocks have been validated, which takes around two weeks, the average time is calculated. If it is too short, the difficulty is increased; if too long, it is decreased.

One of the major issues with PoW is that miners are required to use a lot of computing power. To solve this issue, the Proof of Stake (PoS) process was developed.

Validation by Proof of Stake (PoS)

Validation through PoS is a simpler process than validation through PoW. It enables to both reduce energy demand and make the blockchain more dynamic. This affects the sustainability and economic incentives, as the blockchain will then be able to record transactions more quickly and thus handle a larger volume of transactions.

- The Ethereum project is currently developing a PoS algorithm called Casper. Migration towards Casper should start in 2018 with a hybrid PoS-PoW version, and progressively replace PoW. PoS is expected to speed up the validation of blocks up to more than 20,000 transactions per second.

From a practical perspective, PoS validation is even more decentralised than PoW. Indeed, PoW requires nodes to compete on the same puzzle, creating redundancy in how the computing power is allocated, from the validation of the last transaction to the

moment the puzzle solution is found. Because computing power is unequally distributed, some nodes have more influence than others on the outcome of collective decisions on the blockchain, all the more since much of the computing power used to mine Bitcoins is located in China. The Casper process functions differently: it does not distribute transactions amongst all nodes but divides them into subgroups. The system then favours nodes with the highest engagement, e.g. those with the most Bitcoins, which means that they have the most to lose in case of malicious behaviour. Further, a system of fines exists to punish negative behaviour.

While the PoS system is promising in theory, we do recommend caution: it is currently being tested in Ethereum but is nowhere near as reliable as PoW, which has already withstood large-scale experiments in Bitcoin and Ethereum.

Mining incentives

Mining is an essential part of the blockchain. A gain, or "crypto fuel", that is valued enough is therefore needed to incentivise miners to contribute computing resources and to store the blockchain locally. This compensation needs to offset the economic costs of computing material (required material has very high computing power and/or very high storage capacities), its maintenance as well as energy costs.

As a reminder, miners need a lot of computing power. A compensation is paid for each successful mining operation that is accepted by the peers and added into a block (see "How mining operations are confirmed" in 11.2.).

Blockchain designers define what kind of "crypto fuel" will be produced. It is usually related to the blockchain's activity — bitcoin for the Bitcoin blockchain, ether for the Ethereum blockchain — but can also be designed as part of a loyalty programme: free storage space, computing power, voting power, a car rental, a hotel stay or a trip.

Whichever "crypto fuel" is chosen, the incentive requires a virtual unit that enables miners to accumulate gains depending on how much effort they put in, as a classic loyalty card would do.

11.3. Trust factors

A blockchain consists of several features that can induce trust — however not complete trust.

Decentralised architecture and governance neutrality

Firstly, trust relies on a ***decentralised architecture***, with a large number of nodes belonging to different organisations. Unlike in a centralised architecture where decisions can be taken without consensus, one needs to either produce some level of consensus or control more than 50% of the nodes (or the computing power) to act on the system as a whole. Since the architecture relies on many nodes, the work of validating and storing transactions in the blockchain, as well as any updates to the rules governing the blockchain, need to receive consensus from a broad group of stakeholders, thus forbidding a small group to become too influential in the governance mechanisms.

Trust requires computing resources and storage capacities to be balanced among organisations; yet we observe the exact opposite situation in the Bitcoin blockchain, with the creation of mining pools. The largest three pools have held more than 50% of the network's computing power on several occasions already. This 50% threshold is critical because it enables an organisation or a coalition of organisations to implement a 51% attack: essentially, to be able to control the history of transactions, but not necessarily to steal currency gains nor add malicious transactions.[11]

Secondly, trust relies on a ***neutral governance scheme*** — the blockchain equivalent to the notion of balance of powers. Before investing time and money into a blockchain, one needs to check whether the neutrality of the governance scheme is guaranteed: whether the limited number of people managing the project and its protocol are really independent in their decision-making process and resistant to political or industrial pressure. If such is not the case, then power in the blockchain is fundamentally not balanced. Further, if these stakeholders control more than half of the computing power, the consensus principle does not hold either. Indeed, when the blockchain operating rules are updated through an up-

11 A 51% attack is an attack on the blockchain that filters transactions before the mining process and directs the gains of the mining efforts to its own miners instead of those who are the fastest. In the case of competing blockchains, a group holding more than 50% of the mining power could theoretically allocate their mining power to one of the competing blockchains and therefore decide on the issue of the conflict with confidence.

date of the blockchain's code, miners and their administrators may either accept or reject the update. This can be a minor and backward-compatible update — called a *soft fork* — or a major and not backward-compatible update — called a *hard fork*. To be implemented, a soft fork only requires the support of a majority of miners, whereas a hard fork requires a much larger consensus. In the event a large consensus is not obtained but large-enough groups support both solutions, the blockchain divides into two different blockchains that survive on their own. Therefore, a coalition of stakeholders who hold most of the mining capacity could collude, modify the governance rules, create forks and confusion, create double spending (see below), and risk devaluating the cryptocurrency as a whole.

Transparency enables better auditability

Trust also relies on ***transparency***. This principle applies at many levels, including transactions and algorithms.

- **Traceability and auditability of the entire chain of transactions:** The publication of all transactions recorded from the Genesis Block enables all nodes to verify the integrity of the chain and obtain all the transactions associated with an account. In theory, fraud is therefore impossible: all is public and transparent, in the limits provided by pseudonymity.

- **Algorithmic transparency:** Anybody can read the code used for mining, interacting with the blockchain and implementing a smart contract. This gives experts among the user community the opportunity to scrutinise the code and raise a red flag if they notice anything suspicious. Trust therefore largely relies on watchdogs.

Digital security

Finally, blockchains enable good digital risk management (see Chapter 4) through three main features:

- **A rigid tamper-proof chain:** Both the content of the blocks within the blockchain and their order are tamper-proof. This relies on the decentralised architecture and the consensus principle. On top of this, there can be a mechanism incentivising positive behaviour, disincentivising negative behaviour, and a cryptographic system supporting strong technical guarantees. The PoW relies on consensus and a cryptographic proof that is costly in terms of computing power, while the PoS relies

on consensus and an incentive structure and has not yet proven it could be trusted at a large scale.

- **The ability to authenticate transactions while protecting digital identities:** Blockchains provide privacy (e.g. through the use of pseudonyms) yet implement adapted security measures to guarantee that transactions are valid and that accounts are secure. This balance between identity protection and security management is a crucial factor in trusting the blockchain.

- **Security levels can be tailored:** As new technologies are developed, security mechanisms once deemed trustworthy become vulnerable. To maintain the same level of trust, several blockchains enable security levels to be dynamic.

However, trust in the blockchain can never be complete. Several elements have actually questioned this trust, following these events:

- **Programming errors:** Programmable blockchains imply a high risk of human programming errors, as happened with the 2016 attack on Ethereum. In 4 weeks, the Decentralised Autonomous Organisation (the DAO),[12] which enables its community to invest in venture capital, raised a spectacular amount of $150 million to fuel start-up projects wishing to build over Ethereum. The DAO was then robbed of $50 million by a group of hackers who exploited a vulnerability in the way smart contracts were implemented. This error enabled the attackers to use the function designed to "cash out" an account several times. As Ethereum co-founder Vitalik Buterin wrote in a blog post, "*This is an issue that affects the DAO specifically; Ethereum itself is perfectly safe.*"[13] In 2017, another attack on the wallet software Parity Wallet led to $30 million in ether being stolen..

- **Double spending:** The double spending problem arises when one single piece of currency is used in two different transactions, which should normally exclude each other. This is a voluntary and malicious act, which the mining process deletes under

12 Blockchain France defines a DAO as "*an organisation that relies on a computer software to define rules governing the community. These rules are transparent and immutable, as they are written into the blockchain.*" [Unofficial translation from the French]

13 https://blog.ethereum.org/2016/06/17/critical-update-re-dao-vulnerability/

normal conditions. It can however happen that each mutually exclusive transaction is recorded on a forked chain. In this case, the recipient can only figure out whether they received the transaction once one of the two blockchains is abandoned. For Bitcoin, a reasonable timeframe is 1 hour, i.e. 6 blocks later. The problem of double spending was one of the major issues with online currencies before Bitcoin offered a practical solution to it: the blockchain.

- **Appropriating transactions:** It may be in a miner's interest not to share a transaction with a high fee to other miners. By mining the transaction by himself, the miner ensures they will be the one to receive the transaction fee — but it might take more time for the transaction to get included in the blockchain. This retention attack is becoming more likely as transaction fees are increasing while built-in rewards are decreasing. Similarly, a well-connected miner may choose to retain a block to get more time to mine and broadcast it broadly only when he has received a competitor's block. This type of attacks questions the incentive system and calls for improvements..

- **Money laundering:** Money laundering issues appear every time a new way of exchanging money is created. Contrary to popular belief, transaction transparency does not prevent money laundering; it only makes it more complex. Indeed, some techniques can be used to decrease traceability. Firstly, one can create a multiplicity of accounts (some only used once) and a network of transactions between those accounts. A second approach, called Coinjoin and used in Bitcoin, consists in combining several transactions into a single one. The more transactions are merged (inputs and outputs), the harder it is to link a spender to a recipient. The Zerocash approach we describe in 11.4. guarantees that transactions are non-traceable and makes it impossible to detect money laundering on the sole basis of information acquired from the blockchain.

11.4. Transparency and privacy breaches in the blockchain

A blockchain relies on the pseudonymity of its participants, which means that once the real identity of an account holder is revealed, all of the transactions they made from their account can be revealed. As explained above, many techniques can protect users' real identity, including owning multiple accounts (some only used once) and merging transactions, as is possible with Coinjoin.

The transparency of the blockchain should cause service designers to be more cautious as to the protection of personal data. Indeed, any private information, be it algorithms or data (e.g. personal data, cryptographic keys…), should not be stored unencrypted in the blockchain, for instance in a transaction. However, since it is in any case better to limit the size of the information stored in the blockchain to limit costs, one may still rely on distributed storage systems. Such systems can rely on an externalised, potentially distributed and unlimited memory: they can be implemented to function as a peer-to-peer network[14] (e.g. BitTorrent, GNutella, Napster or Kademlia). In this case, the memory is actually externalised because the content is accessible through a Distributed Hash Table (DHT) key and only this key needs to be referenced in the blockchain.[15] This memory can then store either encrypted or unencrypted data — in the case of encrypted data, there is then a need to manage cryptographic keys.

In 2014, the Zerocash initiative offered an interesting solution for decentralised anonymised payments.[16] This solution enables transparent and untraceable Bitcoin transfers on a blockchain: neither the source, the destination, nor the amount can be inferred. The solution relies on zero-knowledge protocols (where neither party reveals information to the other) that enable a user to prove to a third party they know a secret without having to reveal the secret itself. This relies on zero-knowledge Succinct Non-interactive ARguments

14 A peer-to-peer (P2P) network is a network built over the Internet and made of P2P nodes assigning a portion of their resources for the P2P service, mostly file sharing application, to be provided to the community with the idea that peers are equally privileged and powerful in the application.

15 A DHT key associated to a content can be easily computed by applying a hashing function over the content. This key needs to be known in order to access the associated content stored in a P2P network. To go into detail, the participating P2P nodes share in a distributed way a DHT table including for each entry a DHT key (itself assigned to a content) and a value useful for peers to locate the P2P node where the content is stored. Note that any node is able to compute that value by hashing the DHT key.

16 Ben-Sasson, E., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., Virza, M., (2014). Zerocash: Decentralized Anonymous Payments from Bitcoin, 2014 IEEE Symposium on Security and Privacy.

of Knowledge (zk-SNARKs), particularly efficient since they are able to establish a proof of knowledge in a handful of milliseconds. To explain how this works, the following image is often used: all users pin their banknotes on a wall and remove them when they make a transaction.

Finally, in 2015, the MIT developed a solution called Enigma, which offers a decentralised cloud platform ensuring the confidentiality of all the data processed and the computing operations.[17] It relies on blockchain to ensure the traceability of operations and on the Enigma peer-to-peer network to compute and store sensitive data. The idea is that each Enigma node only possesses an incomplete and meaningless view of the sensitive data being processed, and only processes it partly. Therefore, nodes cannot individually access sensitive information. Through Secure Multi-Party Computing (SMC), they can collaboratively produce the result sought by the system.

11.5. What are the current limits of the blockchain?

We have seen that blockchain technologies have structural limits. They cannot be considered as a basis for complete trust and confidence, even narrowed down to trust. Indeed, organisational issues relating to power dynamics between actors and user appropriation as well as technical factors make studying the actual scope of this technology very complex. However, they indicate once more that mere transparency does not necessarily come with complete trust and an adequate protection of personal data.

Let us finally remind here that Public Key Infrastructures (PKI) were once similarly presented as a revolutionary, trust-inducing technology, before we came to share an understanding of its limits.

Therefore, and as is the case with labels in a broader sense, using a blockchain is a guarantee of certain properties, but should be considered as a way to induce or suggest user trust by emphasizing the appropriate features of this technology.

17 Zyskind, G., Nathan, O., Pentland, A., (2015). Enigma: Enigma: Decentralized Computation Platform with Guaranteed Privacy, http://enigma.media.mit.edu/enigma_full.pdf

How to cite this chapter: Laurent M. “Is blockchain a trustworthy technology?”, *in Signs of trust – The impact of seals on personal data management*, Paris, Handbook 2 Chair Values and Policies of Personal Information, Coordinated by Claire Levallois-Barth, January, 2018, chapter 11, pages 179–197.

http://www.personal-information.org/

Conclusion

Armen Khatchatourov
Claire Levallois-Barth
Maryline Laurent
Patrick Waelbroeck

In this handbook, we addressed the issues raised by a particular kind of trust sign, ***data protection seals***, and we brought to light certain trends that are emerging in the developing digital landscape.

The issue of seals is not a new one — seals have been around for a while in the energy and food industries —, yet digital goods are a specific and skyrocketing market that therefore cannot use solutions already tested elsewhere. The increasing data flows are thus compelling us to reconsider the issue of data protection governance modes in a new light.

In this context, one should certainly consider seals and the related expert intervention as a tool that allows data controllers to gradually increase the level of protection of the data they collect and use. Yet practical modalities still need to be defined. To what extent should companies or professional associations be able to draw up their own benchmarks and audit procedures? We believe including all stakeholders — in particular citizens — in the building process is key, by reshaping the roles of both the regulators and the regulated. We think state intervention is particularly essential on three points: drawing up benchmarks, accrediting certification authorities through existing specialised organisations such as COFRAC, and imposing truly deterrent sanctions to create a healthier market. Indeed, given the substantial possibilities for misuse, some form of pressure is needed to contain companies, even through the mere threat of losing reputation, and therefore trust.

However, as we observed in Chapters 5 and 6 of this handbook, too strict or costly a state intervention may lead stakeholders to turn to private seals, which carry a potentially misleading effect as they provide an embellished picture of data protection. This is undoubtedly a real risk for at least two reasons: first, what used to be a matter for the State now tends (be it rightly or wrongly) to proceed from the private sector; second, the elaboration and issuance of private seals are not regulated enough throughout their life cycles. The fundamental question raised by such signs of trust therefore regards the transfer of policies managing citizens' personal data to the private sector.

On a smaller scale, one may infer that seals are economically useful both for consumers and companies. "Reassuring" customers and potential customers by giving them evidence that digital services are operating well would probably help remove certain barriers. Such observation was confirmed by a survey carried out by the ***Chair Values and Policies of***

Personal Information that polled 2,000 Internet users in March 2017; it showed that informed and experienced users are more likely to consume the most.[1]

Yet, so far, there is no proper data protection business model. Seals, as signs of trust, are necessarily included in companies' marketing strategies (see Chapters 3 and 9), which are meant to allow consumers to assess whether the signal they receive is reliable. Indeed, the signals sent are too numerous and weak to be perceived by consumers and companies. Besides, certification costs range from hundreds to thousands of euros, according to the criteria to be met, the validity period and the chosen audit procedure (see Chapters 6 and 7). It is thus important to reflect on both financial and timely costs. Certification needs to be relatively costly for companies so that seals fulfil their role as signals of best practices in data protection, yet not so pricey that it dissuades companies from getting certified or leads them to increase their prices for those services (see Chapter 9). If companies supported this cost on their own, how could they be encouraged to get certified even as they are unable to determine the return on investment? Conversely, if public certifying organisations took care of it, then how could they support audit costs?

Such questions somehow incite to build certification on technical bases that are supposedly able to establish trust. Yet can technical solutions alone tackle the issue of trust and send a clear and high-quality signal? Are they not merely a risk assessment tool or, at best, a tool that establishes a particular kind of ***trust*** (as opposed to *confidence* in Luhmanns' terminology (see Chapter 1)? Is this risk assessment not relying on criteria that are themselves shaped by stakeholders' competing positions? Indeed, governance processes do not simply consist in displaying external signs of transparency and in implementing this or that technology, be it qualified at a given point in time as *data protection by design*. What we should consider here is the coordination between technologies, their evolution, and governance mechanisms, as shows the example of blockchain (see Chapter 11). Although blockchain may prove reliable and strong from a technical point of view and provide a promising protection through a decentralised system of governance, it should also guarantee that blockchain minors are not controlled by a few central actors. The qualification of a technical solution gives evidence of its technical reliability and strength, yet does not necessarily guarantee they are working well, and only partly gives information on their gov-

1 Waelbroeck, P., Khatchatourov, A., Levallois-Barth, C. (2017) *Synthèse du Rapport « Données personnelles et confiance : quelles stratégies pour les citoyens-consommateurs en 2017 ? »*, Chair Values and Policies of Personal Information, 23 June 2017.

ernance. Far from a static and simplifying vision that would consist in solving governance problems with technical processes, seals bring to the fore a time dimension, by displaying competing economic and political projects.

~

This handbook was essentially dedicated to explaining the conjunction of ***trust*** with a new kind of mechanism we proposed to name "***suggested trust***" (see Chapter 1). It seems, at least as regards the legal framework we described (see Chapters 2 and 9), that users often play a passive part as the addresses of seals; only rarely do they access a more active role by taking part in the suggestion-making process. More grass-roots certification (and trust) mechanisms such as peer-to-peer initiatives should therefore be further considered. For that to happen, users need to be able to assess, in a decentralised way, digital services that use personal data. Yet such assessment would be fundamentally different from the "collaborative" ranking of a hotel or mail order and delivery. There is still much to do in order to create collective seals and audit procedures. It is a huge stake, which implies including citizens and enhancing their sense of belonging to the digital society, and not only to the digital economy.

As a conclusion, the issue of data protection seals raises stakes that we believe are essential and socially ambivalent. On the one hand, individuals are being deresponsibilised, which *de facto* threatens the Enlightenment project and that of autonomous individuals. Unreservedly complying with external orders and signs may lead individuals to lose their necessary critical capacity. For instance, may the generalisation of certification not lead to a generalisation of clear-conscience behaviours or the creation of a new form of user dependence?

On the other hand, individuals are actually being "responsibilised"[2] as they are required to "self-manage" their personal data, for instance through a dashboard included in the software. Consequently, individuals may have to support the costs, as they could be blamed for making transactions through non-certified services, or at least considered to be

2 Here we freely interpret the theme of responsibilisation as brought to the fore by Michel Foucault in a series of lectures he gave at the *Collège de France* in the 1970s, namely "Security, Territory, and Population" and "The Birth of Biopolitics".

creating risks (economic, security, etc.) they should take responsibility for. Individuals are thus held accountable for their choices, yet are not being informed on the ethical, economic and political stakes related to global data flows. Besides, as they comply with the external "trusted" recommendations and suggestions, the impact their punctual choices may have on the constitution of their identity or ability to act is being disregarded.[3]

In a way, what is at stake here is a new paradigm prescribing user behaviour; a profound social tendency: it is no longer about drawing up strict prescriptions forbidding such or such action or behaviour, rather "softer" prescriptions that suggest such or such product or service (see Chapters 1 and 2). "Suggested trust" in digital technologies is nonetheless a proper governance tool.

As a result, data protection seals are a very specific instance of "regulation" as they will lead us to reshape not only the roles of stakeholders (both regulated and regulating) and competition mechanisms, but also and above all the way society envisions social cohesion, at a time where any given individual or collective action creates personal data and is guided by them.

3 See Khatchatourov, A. and Chardel, P.-A. (2016). *La construction de l'identité dans la société contemporaine : enjeux théoriques. in « Identités numériques », Cahier n°1 de la Chaire Valeurs et Politiques des Informations Personnelles*, coordinated by Claire Levallois-Barth.

How to cite this chapter: Khatchatourov A., Levallois-Barth C., Laurent M., Waelbroeck P. “Conclusion”, *in Signs of trust – The impact of seals on personal data management*, Paris, Handbook 2 Chair Values and Policies of Personal Information, Coordinated by Claire Levallois-Barth, January, 2018, pages 199–203.

http://www.personal-information.org/

Appendices

Tables and figures

Index

A

B

C

D

E

F

G

H

I

K

L

M

N

P

Q

R

S

T

U

V

W

List of abbreviations

AFCDP	*Association Française des Correspondants à la protection des Données Personnelles* — French Association of Data Protection Officers
AFNOR	*Association française de Normalisation* — French Standardization Association
ANSSI	*Agence Nationale de la Sécurité des Systèmes d'Information* — National Agency for the Security of Information Systems
Art.	Article
BBB	Better Business Bureau
CA	*Cour d'Appel* — French Court of appeal
Cass.	*Cour de cassation* — French Court of *Cassation*
CCRA	Common Criteria Recognition Arrangement
CSPN	*Certificat de Sécurité de Premier Niveau* — First Level Security Certificates
CE / EC	*Communauté Européenne* — European Community
CEN	*Comité Européen de Normalisation* — European Committee for Standardization
CENELEC	*Comité Européen de Normalisation en ÉLECtronique et en électrotechnique* — European Committee for Electrotechnical Standardization
CESTI	*Centre d'Évaluation de la Sécurité des Technologies de l'Information* — Centre for Evaluation of the Security of Information Technology
Cf.	*Confer*
CISPE	Cloud Infrastructure Service Providers in Europe
CNIL	*Commission Nationale de l'Information et des Libertés* — National Commission on Informatics and Liberty, the national data protection authority for France.
COFRAC	*COmité FRançais d'ACcréditation* — French Accreditation Committee
coll.	collection
Crim.	*Chambre criminelle* — French Criminal Chamber
D.	*Dalloz* — a French publisher that specializes in legal matters and is France's main legal publisher.
DAO	Decentralized Autonomous Organisation
DHT	Distributed Hash Table
DPO	Data Protection Officer
EAL	Evaluation Assurance Level
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
ECOJ	Official Journal of the European Community
EDPB	European Data Protection Board

eIDAS	Electronic IDentification And trust Services
eIDAS Regulation	Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation) adopted on 23 July 2014.
ESRB	Entertainment Software Rating Board
EU	European Union
EUOJ	Official Journal of the European Union
FDPIC	Federal Data Protection and Information Commissioner
FEVAD	*FEdération du e-commerce et de la Vente À Distance* — French Federation of E-commerce and Distance Selling
FNTC	*Fédération des Tiers de Confiance du numérique* — French Trusted Third Parties Federation
FTC	Federal Trade Commission
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
ISO	International Organization for Standardization
LCEN	*Loi pour la Confiance dans l'Économie Numérique* — French Law on Confidence in the Digital Economy
No	number
OJ of the French Republic	Official Journal of the French Republic
p.	page
PKI	Public Key Infrastructure
PoW	Proof of Work
PoS	Proof of Stake
RLDI	*Revue Lamy Droit de l'Immatériel*
RSA	Rivest Shamir Adleman
SHA	Secure Hash Algorithm
SOG-IS	Senior Officials Group Information Systems Security
SQS	Swiss Association for Quality and Management Systems
ToE	Target of Evaluation
UBA	User Behaviour Analytics
ULD	*Unabhängiges Landeszentrum fuer Datenschutz* — Data protection authority for the German Land Schleswig-Holstein.
WP29	Article 29 Data Protection Working Party

List of interviews conducted from October 2015 to September 2017

By Claire Levallois-Barth and Delphine Chauvet

Arnaud Belleil, Digital Transformation Director, Cecurity.com

Maître Alain Bensoussan, Attorney, Alain Bensoussan Avocats

Jérôme Beranger, Co-founder and Chief Strategy Officer, ADEL

Florent Bonnet, CIL Consulting

Johanna Carvais, Privacy Seals Manager, and Valérie Bourriquen, Lawyer, CNIL

Maître Etienne Drouard, Associate Attorney, K&L Gates

Eric Lachaud, PhD Candidate in Law Technology, Tilburg Institute for Law, Technology, and Society (TILT), Tilburg University, Netherlands

Maître Denise Lebeau-Marianna, Associate Lawyer, DLA Piper France LLP

Xavier Leclerc, CEO, Axil-Consulting

Maître Nathalie Metallinos, Associate Lawyer, IDEA Avocats

Laurent Midrier, VP for Strategy and Innovation, Bureau Veritas

Hervé Molina, IT Audit Director, and **Jean-Christophe Carbonel**, Head of Audit, Global Security Manager, Le Groupe La Poste

Maître Fabrice Naftalski, Associate Lawyer, EY

Maître Yann Padova, Associate Lawyer, Baker & McKenzie (Paris), former Commissioner in charge of Data Protection (2015-2017) at the French Energy Regulatory Commission (*Commission de régulation de l'énergie* — CRE), and former Secretary General of the CNIL (2006-2012)

Benoît Pellan, Digital Product Manager, Innovation & Development Section, AFNOR Certification

Bruno Rasle, Executive Officer, French Association of Data Protection Officers (*Association Française des Correspondants à la Protection des Données* — AFCDP)

Frédéric Richter, CEO, Stiftung Datenschutz, Germany

Stéphane Schmoll, CEO, and **Laurent Cellier**, User Experience Director and Data Protection Officer, Deveryware

Maître Thibault Verbiest, Associate Lawyer, De Gaulle Fleurance & Associés

Cécile Wendling, Head of Foresight, AXA

Delphine Zberro, Director - IT Advisory, Deloitte

Bibliography

Acquisti, A. (2012). Nudging Privacy: The Behavioral Economics of Personal Information. *in Jacques Bus, Malcolm Crompton, Mireille Hildebrandt, George Metakides (eds), Digital Enlightenment Yearbook 2012*, IOS Press.

Agosti, P., Caprioli, E.A., (2005). La confiance dans l'économie numérique (Commentaires de certains aspects de la loi pour la confiance dans l'économie numérique) (LCEN), Petites affiches, 03/06/2005, n°110.

Akerlof, G. A. (1970). The market for lemons : Quality uncertainty and the market mechanism. The quarterly journal of economics, 488-500.

Anton, A., Earp, J. B., Bolchini, D., He, Q., Jensen, C., Stufflebeam, W. (2003). The lack of clarity in financial privacy policies and the need for standardization. IEEE Security & Privacy, 2(2):36-45. DOI : 10.1109/MSECP.2004.1281243.

Bakos, Y., Marotta-Wurgler, F., Trossen, D. R. (2014). Does anyone read the fine print? Consumer attention to standard-form contracts. The Journal of Legal Studies, 43(1), 1-35. DOI : 10.1086/674424.

Barabàsi, AL. (2002). Linked: The New Science of Networks, Perseus, Cambridge, MA.

Becher, S. I., Zarsky, T. (2015). Online Consumer Contracts: No One Reads, But Does Anyone Care?

Ben-Sasson, E., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., Virza, M., (2014). Zerocash: Decentralized Anonymous Payments from Bitcoin, 2014 IEEE Symposium on Security and Privacy.

Bjørner, T. B., Hansen, L. G., & Russell, C. S. (2004). Environmental labeling and consumers' choice—an empirical analysis of the effect of the Nordic Swan. Journal of Environmental Economics and Management, 47(3), 411-434. DOI : 10.1016/j.jeem.2003.06.002.

Brounen, D., Kok, N. (2011). On the economics of energy labels in the housing market. Journal of Environmental Economics and Management 62(2):166-179. DOI : 10.1016/j.jeem.2010.11.006.

Cabral, L, Hortascu, A. (2010). Dynamics of Seller Reputation : Theory and Evidence from eBay, Journal of Industrial Economics, v. 58, no.1, March 2010, pp. 54-78

Carvais, J. (2015). Le label CNIL comme outil de conformité, *in AFCDP, Correspondant Informatique et Libertés, Bien plus qu'un métier*. pp. 497 à 510.

Castets-Renard, C., (2006). Le formalisme du contrat électronique ou la confiance décrétée, Defrénois, 30/10/2006, n° 20, p. 1529.

Chochois, M., Magnin, N., (2015). Qualité des produits de SSI, les labels français, Techniques de l'ingénieur, H5825 v2, octobre 2015.

Connolly, C. (2008). Trustmark Schemes Struggle to Protect Privacy, Working paper.

Connolly, C., Greenleaf, G. and Waters, N. (2014). Privacy self-regulation in crisis? TRUSTe's 'deceptive' practices, 132 Privacy Laws & Business International Report, 13-17, December 2014.

Cornu, G., (2016). Vocabulaire juridique, Paris, PUF, 11e édition, 2016, V° Confiance.

Foucault, M. (2004). Naissance de la biopolitique, Paris, Gallimard/Le Seuil, coll. « Hautes Études ».

Fournier, P. (2015). La responsabilité comme mode de gouvernement néolibéral : l'exemple des programmes d'aide aux familles aux États-Unis de 1980 à nos jours. *in Les ateliers de l'éthique*, Volume 10, Numéro 1.

Gao, Z. (2007). Effects of additional quality attributes on consumer willingness-to-pay for food labels (Doctoral dissertation, Kansas State University).

Khatchatourov, A. (2016) Big Data entre archive et diagramme. Études Digitales n°2, Classiques Garnier, Paris.

Khatchatourov, A. (2016). Peut-on mettre la main sur les algorithmes? Note sur la «culture algorithmique» de Dourish. Études Digitales, n°2, Classiques Garnier, Paris.

Khatchatourov, A. et Chardel, P.-A. (2016). La construction de l'identité dans la société contemporaine : enjeux théoriques. *in «Identités numériques»*, Cahier n°1 de la **Chaire Valeurs et Politiques des Informations Personnelles**, coordonné par Claire Levallois-Barth.

Kiesel, K., Villas-Boas, S. B. (2007). Got organic milk? consumer valuations of milk labels after the implementation of the USDA organic seal. Journal of agricultural & food industrial organization 5(1). DOI : 10.2202/1542-0485.1152

Lachaud, E., (2016). Could the CE Marking Be Relevant to Enforce Privacy by Design in the Internet of Things? *In Data Protection on the Move* (pp. 135-162). Springer Netherlands.

Lachaud, E., (2016). Why the certification process defined in the General Data Protection Regulation cannot be successful. Computer Law & Security Review 32, 814–826.

Lachaud, E. (2017). The General Data Protection Regulation and the rise of certification as a regulatory instrument. Computer Law & Security Review.

LaRose, R. and Rifon, N., (2007). Promoting i-Safety: Effects of Privacy Warnings and Privacy Seals on Risk Assessment and Online Privacy Behavior (Summer 2007), vol. 41, Journal of Consumer Affairs 12.

Laurent, M., et Kaâniche, N. (2016). Les preuves d'identités ou d'attributs préservant le pseudonymat. *in « Identités numériques »*, Cahier n°1 de la **Chaire Valeurs et Politiques des Informations Personnelles**, coordonné par Claire Levallois-Barth.

Leire, C., Thidell, Å. (2005). Product-related environmental information to guide consumer purchases–a review and analysis of research on perceptions, understanding and use among Nordic consumers. Journal of Cleaner Production, 13(10), 1061-1070. DOI : 10.1016/j.jclepro.2004.12.004.

Leon, P. G., Faith Cranor, L., McDonald, A. M., and McGuire, R., (2010). Token attempt: The Misrepresentation of Website Privacy Policies Through the Misuse of P3P Compact Policy Tokens, CyLab. Paper 73.

Levallois-Barth, C., Meseguer, I. (2016). Privacy Shield: un bouclier à peine brandi déjà ébréché?, Éditorial de la lettre d'information trimestrielle n° 5 de la **Chaire Valeurs et Politiques des Informations Personnellles**, décembre 2016.

Levallois, C. (2016). Identités numériques et gestion des données personnelles. *in « Identités numériques »*, Cahier n°1 de la **Chaire Valeurs et Politiques des Informations Personnelles**, coordonné par Claire Levallois-Barth.

Levallois, C. (2016). La réglementation mise en place par l'Union européenne en matière d'identification électronique et des services de confiance (règlement eIDAS). *in « Identités numériques »*, Cahier n°1 de la **Chaire Valeurs et Politiques des Informations Personnelles**, coordonné par Claire Levallois-Barth.

Levy, A. S., Mathews, O., Stephenson, M., Tenney, J. E., & Schucker, R. E. (1985). The impact of a nutrition information program on food purchases. Journal of Public Policy & Marketing, 1-13.

Li, Q., Curtis, K. R., McCluskey, J. J., & Wahl, T. I. (2003). Consumer attitudes toward genetically modified foods in Beijing, China.

Loureiro, M. L., McCluskey, J. J. (2000). Consumer preferences and willingness to pay for food labeling: A discussion of empirical studies. Journal of Food Distribution Research 34(3):95-102.

Luhmann, N. (2001). Confiance et familiarité: Problèmes et alternatives. Réseaux, no 108,(4), 15-35. doi:10.3917/res.108.0015. Traduction de Louis Quéré.

Luhmann, N. (2010). Le Pouvoir [« Macht »], Presses de l'Université Laval, 1975 / 2010.

Machina, M., (2007). Non-expected Utility, *in Darity (Ed), International Encyclopedia of the Social Sciences*, Macmilan Reference USA, 2nd Edition.

Mai B, Menon N M, Sarkar S (2010) No free lunch: Price premium for privacy seal-bearing vendors. Journal of Management Information Systems 27(2):189-212.

Mantelero, A. (2013). Competitive value of data protection: the impact of data protection regulation on online behavior, International Data Privacy Law 3(4): 229-238. DOI : 10.1093/idpl/ipt016.

McDonald, A. M., Cranor, L. F. (2009). The cost of reading privacy policies. ISJLP, 4, 543.

Mekki, M., (2009). Propos introductifs sur le droit souple, in Le droit souple, Dalloz, Coll. « Thèmes et commentaires ».

Melnik, M. I., & Alm, J. (2002). Does a seller's ecommerce reputation matter? Evidence from eBay auctions. The journal of industrial economics, 50(3), 337-349. DOI : 10.1111/1467-6451.00180.

Miyazaki, A. D., Krishnamurthy, S. (2002). Internet seals of approval: Effects on online privacy policies and consumer perceptions. The Journal of Consumer Affairs 28-49. DOI : 10.1111/j.1745-6606.2002.tb00419.x.

Moore, T., Anderson, R. (2012). Internet security. The Oxford Handbook of the Digital Economy'(Oxford University Press 2011).

Naftalski F.et Desgens-Pasanau G., (2010). Enjeux et perspectives du pouvoir de labellisation de la CNIL, Revue Lamy Droit de l'Immatériel, N°63, août-septembre 2010, 12 pages.

Naftalski, F. (2011). Label CNIL et conformité « informatique et libertés » : publication des premiers référentiels, Revue Lamy Droit de l'Immatériel.

Noussair, C., Robin, S., Ruffieux, B. (2002). Do consumers not care about bio-tech foods or do they just not read the labels? Economics letters, 75(1), 47-53. DOI : 10.1016/S0165-1765(01)00594-8.

Olurin, M., Adams, C., Logrippo, L. (2012). Platform for privacy preferences (p3p): Current status and future directions. IEEE, Tenth Annual International Conference on Privacy, Security and Trust (PST), pp 217-220. DOI : 10.1109/PST.2012.6297943.

O'Neil. (2014). Hacking Weber: Legitimacy, critique, and trust in peer production.

Parasuraman, R., Mouloua, M., & Molloy, R. (1996). Effects of adaptive task allocation on monitoring of automated systems. *in Human Factors: The Journal of the Human Factors and Ergonomics Society*.

Pasquale, F. (2015). The Black Box Society: The Secret Algorithms That Control Money and Information, Harvard University Press.

Penneau, A. (2014). Certification et codes de conduite privés : article 38 et 39 (dans leur version originelle), *in La proposition de règlement européen relatif aux données personnelles : propositions du réseau Trans Europe Experts*, sous la direction de Nathalie Martial-Braz, Société de législation comparée, volume 9, 2014, p. 351.

Pontier, J.-M. , (1996). La certification, outil de la modernité normative.

Quéré, L. (2001). La structure cognitive et normative de la confiance.

Rodrigues, R., Wright, D. and Wadhwa, K. (2013). Developing a privacy seal scheme (that works), International Data Privacy Law Advance Access, published February 1, 2013, 17 pages,. p. 15.

Rodrigues, R., Barnard-Wills, D., Wright, D., De Hert, P., Papakonstantinou, E. (2013). EU Privacy seals project: Inventory and analysis of privacy certification schemes. Final Report. Publications Office of the European Union.

Rouvroy, A. & Berns, T. (2013). Gouvernementalité algorithmique et perspectives d'émancipation : le disparate comme condition d'individuation par la relation. Réseaux 31.

Stiegler, B. (2015). La Société automatique. L'avenir du travail, Fayard.

Tambou, O., (2016). L'introduction de la certification dans le règlement général de la protection des données personnelles : quelle valeur ajoutée ?, Revue Lamy de Droit de l'Immatériel, avril 2016, pp. 51-54.

Vivant, M., (2004). Entre ancien et nouveau, une quête désordonnée de confiance pour l'économie numérique, Cahier Lamy Droit de l'informatique et des réseaux, n°171, juillet 2004, p. 2 et s.

Waelbroeck, P., Khatchatourov, A., Levallois-Barth, C. (2017) Synthèse du Rapport « Données personnelles et confiance : quelles stratégies pour les citoyens-consommateurs en 2017 ? », **Chaire Valeurs et Politiques des Informations Personnelles**, 23 juin 2017.

Zyskind, G., Nathan, O., Pentland, A., (2015). Enigma: Enigma: Decentralized Computation Platform with Guaranteed Privacy.

Talks given by members of the Chair on Signs of trust and seals (External events)

8 December 2017 • **Armen Khatchatourov** took part in the panel **"Defining and managing risks for personal data in information systems"** during a Study Day on the topic "Privacy, personal data and risks: which parameters can enable them to coexist?"; ENS, Paris, France.

8 November 2017 • **Claire Levallois-Barth** gave a talk on "Signs of trust" at the conference on **"Trust in action: trust, digital technologies and design"** organised by the Fondation Mines-Télécom, Paris, France.

5 October 2017 • During the event on **Connected Health Devices** organised by the IMT in Paris, France, **Armen Khatchatourov** led the panel discussion "Data measurement and quality" and **Maryline Laurent** led the panel discussion "Trust and security", in which **Claire Levallois-Barth** took part.

10 May 2017 • **Maryline Laurent** took part in the **panel discussion on "What is left of trust in the digital age?"** and talked about signs of trust in computer science, during a breakfast organised by the Fondation Mines-Télécom, NUMA, Paris, France.

28 April 2017 • During a **Study Day on "The legal framework applicable to the processing of personal data"** organised by the CERAPS (UMR 8026) Research Centre and Université de Lille as part of the ANR "APPEL" research project, in Lille, France, **Claire Levallois-Barth** gave a talk on the topic "How can seals improve the effectiveness of the legal framework applicable to the processing of personal data?"

29 March 2017 • During an event on **"Distributed trust in the digital age"** organised by the Fondation Mines-Télécom, at the WAI BNP Paribas, Paris, France, **Armen Khatchatourov** talked about "Trust in digital environments" and **Claire Levallois-Barth** about "Regulated trust: the example of data protection seals."

Internal events organised by the Chair on the topic of signs of trust (for partners only)

20 November 2017 • **Presentation at Orange Labs, Châtillon, France**

During this meeting, **Claire Levallois-Barth**, **Armen Khatchatourov**, **Maryline Laurent** and **Patrick Waelbroeck** shared their insight on signs of trust according to their field of research.

15 March 2017 • **Presentation in front of the CNIL Certification Committee**

During this meeting, **Claire Levallois-Barth** presented the results of the research conducted on data protection seals. Various forms of action on the part of supervisory authorities were discussed with CNIL Commissioners and the Chair's cross-disciplinary team.

14 March 2017 • **In-house Working Group on GDPR**

Clément Chevauché, of AFNOR Normalisation, introduced and discussed a document entitled "Voluntary standards in digital technologies: a real asset."

15 December 2016 • **In-house workshop on "Data protection seals: what kind of trust do they induce?"**

This workshop was meant to define both the meaning of trust and its social role. **Claire Levallois-Barth** explained that the concept of trust found itself between comprehensive knowledge and the lack of knowledge and thus was aimed at filling this gap between experts and non-specialists. She also set out the GDPR provisions on certification and seals. **Armen Khatchatourov** presented a criticism of the role of trust as risk management.

16 December 2015 • **In-house workshop on "Data protection seals, law and economics: a state of the art"**

During this workshop, **Delphine Chauvet** and **Claire Levallois-Barth** tried to define the notions of seal, certification, trust mark and approval in the frame of the French and European laws. They presented the latest developments in data protection seals and questioned the reasons why the hundred seals that were already listed had not yet acquired visibility from the public. **Patrick Waelbroeck** and **Antoine Dubus** discussed the economic feasibility of data protection seals.

30 April 2014 • **In-house workshop on "Issues raised by data protection certification"**

This workshop, facilitated by **Claire Levallois-Barth**, provided first insight on data protection certification through a presentation by **Arnaud Belleil**, Associate Director, Cecurity.com, on the stakes and problems of certification, and another by **Matthieu Grall**, Head of the Technology Experts Department, CNIL, entitled "Certification in the eyes of the CNIL, ANSSI and the ISO."

The Chair Values and Policies of Personal Information

Founded in March 2013 by the Institut Mines-Télécom, the Chair gathers a cross-disciplinary team of researchers who work on the legal aspects of regulation and compliance, technical aspects of systems and data security, economic aspects of the sharing of personal information, and philosophical aspects of the responsibility and anticipation of societal consequences.

The Chair is sponsored by seven organisations: six founding sponsors, i.e. Groupe Imprimerie Nationale, BNP Paribas, Orange, LVMH, QWANT, SOPRA STERIA, and one associate sponsor, Dassault Systèmes. It works with the CNIL (French Data Protection Authority) and the French Inter-ministry Direction for Digital and ICT Systems (DINSIC), and is supported by the Fondation Mines-Télécom.

The Chair is coordinated by Claire Levallois-Barth, Associate professor of Law at Télécom Paris Tech, and was co-founded with Ivan Meseguer, European Affairs, Research and Innovation Direction of the Institut Mines-Télécom; Maryline Laurent, Professor of Computer Science at Télécom SudParis; Patrick Waelbroeck, Professor of Economics at Télécom ParisTech; and Pierre-Antoine Chardel, Professor of Social Philosophy at the Télécom Management School.

The Chair aims to help companies, citizens and public authorities to reflect on the collection, use and sharing of personal information, i.e. information about individuals (their personal lives, their professional activities, their digital identities, their contributions on social networks, etc.), including those collected by smart objects that surround them. This information, be it directly provided by individuals or indirectly through traces of activity or interaction, brings about many questions as regards social value, economic value, monitoring policy, and regulation policy.

The Chair's works are carried out along 5 cross-disciplinary research focuses:

- digital identities;
- management of personal information;
- contribution and traces;
- personal information in the Internet of Things;
- personal information policies.

Beside publishing research articles and taking part in symposiums and conferences, the Chair organises open events on a regular basis to raise awareness in the greater public on major digital stakes.

MORE INFORMATION

www.personal-information.org
youtube.informations-personnelles.org
@CVPIP

CONTACT

CLAIRE LEVALLOIS-BARTH
Chair Coordinator
claire.levallois@imt.fr

ANNE-CATHERINE AYE
Chair Assistant
cvpip@imt.fr
+33 1 45 81 72 53

Télécom ParisTech - IMT
46 rue Barrault | F-75634 Paris Cedex 13 - France

Authors

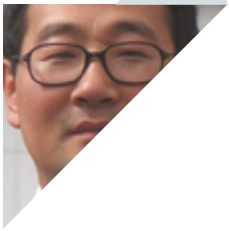
Claire Levallois-Barth

Associate Professor of Law at Télécom ParisTech and Chair coordinator. Her studies focus on the evolution of the protection of fundamental liberties and rights in the digital era, especially on personal data protection in the context of Big Data and digital identity management.

Armen Khatchatourov

Research fellow and Doctor of Philosophy (Philosophy of technics) at the Télécom Management School. By coordinating a theoretical approach with engineering, he focuses on how digital technologies impact on one's sense of self and on the consequences of such technologies on social cohesion.

Patrick Waelbroeck



Professor of Economics at Télécom ParisTech and co-founder of the Chair.
His works focus on innovation economics, the economics of intellectual property, Internet economics and the economics of personal data. He teaches Internet economics and the economics of personal data.

This handbook has been translated from French by Claire Harris and Hugo Zylberberg.
Cécile Hervet was in charge of Chapters 3, 9 and 10.

Maryline Laurent

Professor of Computer Science at Télécom SudParis and co-founder of the Chair. Head of the R3S team (Réseaux, Systèmes, Services, Sécurité - Networks, Systems, Services and Security) at the UMR 5157 SAMOVAR laboratory. She studies the issues of security and privacy in Cloud environments and miniaturised systems as well as digital identity management.

Delphine Chauvet

Postdoctoral researcher in Law at Télécom ParisTech. She defended a thesis on “Privacy. A study of private law.” at Université Paris-Sud and is now a teacher at Université Paris 2 Panthéon-Assas.

Antoine Dubus

PhD researcher in Economics at the Chair Values and Policies of Personal Information. He studies the topic “Data protection and competition.” His studies focus especially on selling data for ad targeting, online personalised recommendation, and targeting through pricing.

With contributions from Ivan Meseguer, co-founder of the Chair, European Affairs, Research and Innovation Direction of the Institut Mines-Télécom, and Chantal Friedman and Anne-Catherine Aye, Chair Assistants.

Trust, as the foundation of any society, questions the very existence of institutional and commercial exchanges and the role these exchanges play in building a cohesive social body. Yet, we are currently experiencing an obvious crisis of trust, enabled by digital technologies.

Economics and computer science both rely on the notion of risk; the former in transactions and the latter in the security of technical systems. In law, trust is usually defined as the belief in one's good faith. From a socio-philosophical perspective, trust is one of the main uncertainty-reducing mechanisms in our complex modern society Yet, to reduce complexity, a conceptual distinction is made between declared trust and assured trust (or confidence).

In this handbook, we address the issue of data protection seals as trust enablers. What impact do seals have on user perception and consumption? How might technologies, including blockchain, be helpful? What is and what should be the State's role? Might the omnipresence of seals and of trust by design not come with limitations? Will overusing seals not lead to disempowering individuals by releasing them from critical analysis?

Partners of the Chair Values and Policies of Personal Information

FOUNDING SPONSORS

GROUPE Imprimerie Nationale

BNP PARIBAS

orange

LVMH

sopra steria

Qwant

ASSOCIATE SPONSOR

DASSAULT SYSTEMES

ACCREDITED/ QUALIFIED PARTNERS

CNIL. Commission Nationale de l'Informatique et des Libertés

DINSIC*

*French Inter-ministry Direction for Digital and ICT Systems

Nereïs – 06 62 12 15 25 – www.nereus.fr – RCS 499 438505