Protection de la vie privée

Guillaume Piolle
guillaume.piolle@supelec.fr
http://guillaume.piolle.fr/

Supélec, campus de Rennes

17 avril 2014 – Formation ISN

Ce qui est privé est-il honteux ?

Si vous n'avez rien à vous reprocher, alors vous n'avez rien à cacher.

- Mais alors, pourquoi utiliser une enveloppe lorsque vous envoyez une lettre ?
- Ce n'est pas parce que vous n'avez « rien à cacher » que rien ne pourra vous être reproché ou que rien ne pourra vous blesser.

Ce genre de déclaration est habituellement faite par un membre d'une « caste dominante » : un homme, blanc, hétérosexuel, si possible de plus de 45 ans.

Les risques : la brèche de vie privée

Formes principales

- Intrusion d'une personne dans vos affaires « privées » ;
- Révélation au public ou à un tiers d'une information « privée » que vous n'étiez pas prêt(e) à divulguer, et/ou qui est fausse ;
- Vol d'identité.

Conséquences possibles

- Impact (plus ou moins grave) sur les relations sociales ;
- Risque de discrimination ;
- Risque de poursuites pénales ;
- ...

Et les personnes « publiques » ?

Les risques : Le vol d'identité

Symptômes (`identitytheft.org.uk`)

- Perte de papiers d'identité ;
- Les courriers (banque notamment) ne vous parviennent plus ;
- Opérations bancaires inhabituelles ;
- On vous informe que vous avez fait une demande de prêt, d'aide sociale ou gouvernementale ;
- Vous recevez des factures, injonctions de payer ou mises en demeures pour des biens ou services dont vous n'avez pas connaissance ;
- On vous refuse un crédit alors que vous avez un bon dossier ;
- Un contrat de téléphonie mobile a été souscrit en votre nom ;
- Vous êtes contactés par des organismes bancaires avec lesquels vous n'avez pas de contacts habituellement ;
- ...

Quel rapport avec l'informatique ?

La notion de vie privée, de droit à la vie privée, de protection de la vie privée. . . peut être considérée indépendamment de l'informatique

L'informatique (et Internet) apporte de **nouvelles sources de risques** mais également de **nouveaux outils de protection**.

Services web, *Cloud computing* et vie privée : Mat Honan

L'affaire Mat Honan

Journaliste *senior* du magazine *Wired*.
En août 2012, la totalité de ses comptes en ligne sont compromis et une grande partie de ses données sont détruites par quelques attaquants.

Mat Honan, *How Apple and Amazon Security Flaws Led to My Epic Hacking* (`http://www.wired.com/gadgetlab/2012/08/apple-amazon-mat-honan-hacking/all/`), Wired, 6 août 2012.

Les dégâts

- Compte Google compromis puis supprimé ;
- Compte Twitter compromis et utilisé pour diffuser des propos racistes et homophobes ;
- Compte Amazon compromis ;
- Compte AppleID compromis, permettant la suppression à distance de données sur ses iPhone, iPad et MacBook (une année de photos, 8 ans de messagerie Gmail).

Services web, *Cloud computing* et vie privée : Mat Honan

La motivation du hacker ?

Le contrôle de son compte Twitter, `@mat`, convoité car en trois caractères. . .

Les causes du désastre

- Liens systématiques entre les différentes identités ;
- Pas d'authentification à deux facteurs ;
- Pas de stratégie de sauvegarde efficace ;
- Applications Apple conçues pour contrôler les données de l'utilisateur depuis un service central (design « aggressif » pour la vie privée) ;
- Failles critiques dans les procédures de sécurité d'Amazon et Apple (un numéro de carte de crédit partiel affiché par Amazon et utilisé comme facteur d'authentification par Apple).

Services web, *Cloud computing* et vie privée : Mat Honan

Ce qui a pu être récupéré

Reprise de contrôle des comptes en ligne, restauration de la plupart des données *cloud* (Gmail et compagnie), effacement du MacBook interrompu, essentiel des données récupéré.

Chez Mat Honan

Mise en place d'une réelle stratégie de sauvegarde, systématisation de l'authentification à double facteur, désactivation des services *Find my* d'Apple.

Chez Amazon

Correction de la faille organisationnelle

Chez Apple

Aucune info sur les modifications de procédure... Les hackers considèrent toujours les comptes AppleID comme des portes ouvertes...

La vie privée : une notion liée à la culture

En France

Droit fondamental, et même « fondamental fondamental », condition nécessaire à l'exercice des autres droits fondamentaux.
Dans le bloc constitutionnel depuis 1971.
Rôle central de l'État comme garant de ce droit.

Aux États-Unis

Ne peut entrer en conflit avec la liberté d'expression, juridiquement supérieure (premier amendement).
Défiance envers l'État.
Rôle central du marché, de la libre entreprise.

Historique

- Warren & Brandeis 1890 : *The Right to Privacy*. Premières réflexions suite aux progrès de la photographie ;
- Création progressive d'un droit à la vie privée dans la doctrine juridique, sous la forme d'un **droit de propriété incorporelle** lié aux **droits de la personne** ;
- 1970 : introduction du droit à la vie privée dans le Code civil français ;
- Fin des années 1970 : Scandale du fichier Safari, loi Informatique et Libertés ;
- Années 1990 et 2000 : trop denses pour être résumées ici !

Historique

Rappel :

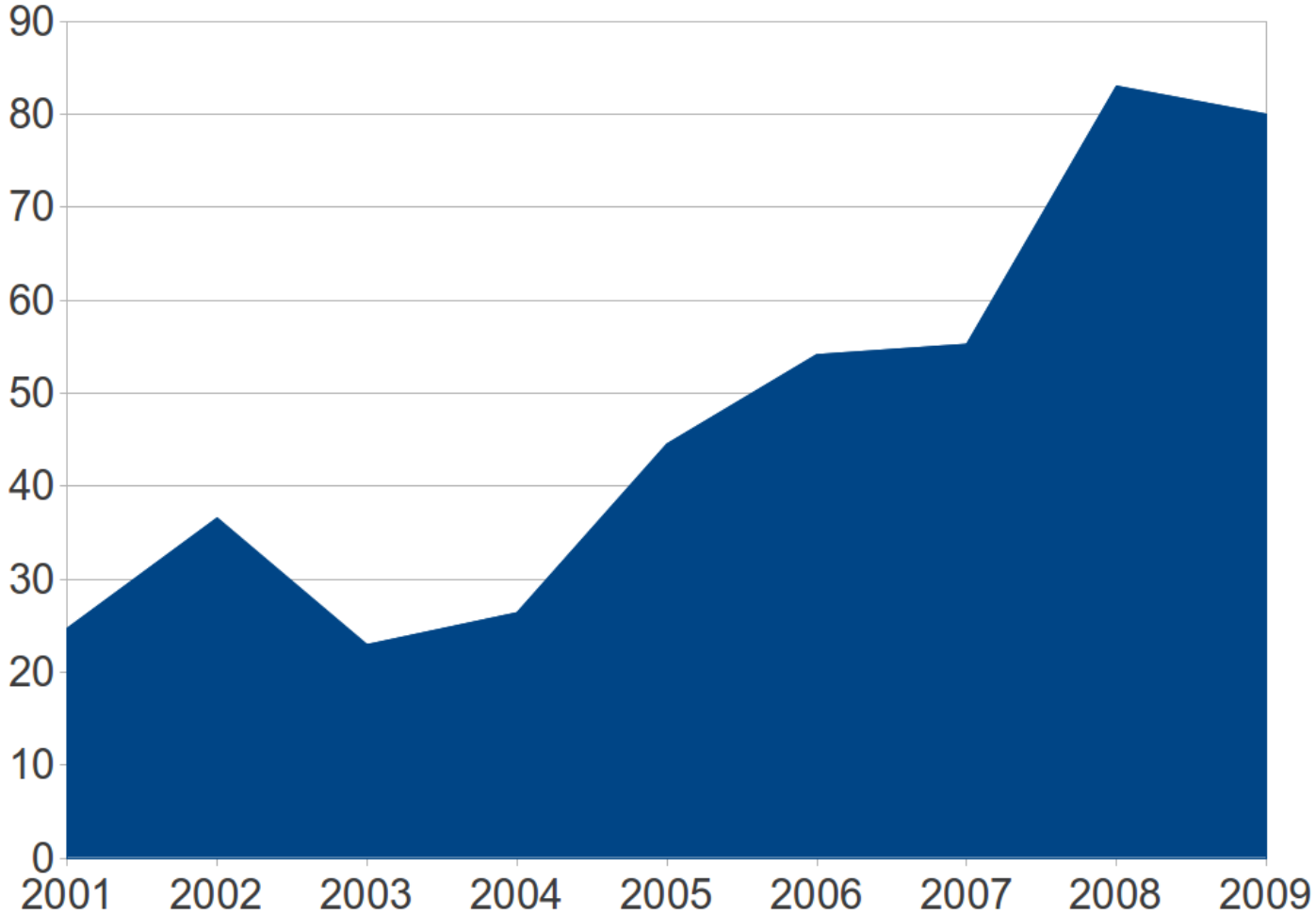
Historiquement, « l'ennemi » n'est pas Google, c'est l'État !

Depuis les années 2000, les inquiétudes liées à la vie privée se tournent vers d'autres acteurs.

Est-ce parce qu'il n'est plus nécessaire de se méfier de l'État ?

- Le fichier Safari a été réintroduit (Edvirsp dans la loi Loppsi 2, et il a de nombreux petits camarades (44 nouveaux entre 2002 et 2009) ;
- Nombreux fichiers illégaux à l'Intérieur et à la Défense (cf période de grâce après 2004) ;
- Accès abusifs aux fichiers ;
- ...

Historique



Taux d'erreurs du fichier STIC (source : J.-M. Manach)

Droit à la vie privée *vs* Protection des données personnelles

Droit à la vie privée

Droit « correctif »
Notion de préjudice et de réparation
Il faut démontrer le préjudice

Protection des données personnelles

Droit « préventif »
Règles visant à éviter les violations de la vie privée
La violation des règles constitue un préjudice en soi, par principe

Périmètre et acteurs

Donnée à caractère personnel (donnée personnelle)

Extrait de l'article 2 :

Constitue une donnée à caractère personnel **toute information relative à une personne physique identifiée ou qui peut être identifiée**, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer **l'ensemble des moyens** en vue de permettre son identification dont dispose ou auxquels peut avoir accès **le responsable du traitement ou toute autre personne**.

Avant 2004 (cf directive 95/46), on parle d'*informations nominatives* ou *indirectement nominatives*.

Périmètre et acteurs

Les acteurs décrits par la loi

- Le responsable de traitement ;
- La personne concernée (sujet des données) ;
- Les destinataires ;
- Les sous-traitants ;
- La CNIL ;
- Le CIL.

Principe de légalité

Traitements interdits

- Origines raciales ou ethniques ;
- Opinions politiques, philosophiques, religieuses ;
- Appartenance syndicale ;
- Santé et vie sexuelle.

Exceptions : consentement exprès, sauvegarde de la vie humaine, gestion des listes de membres, données déjà rendues publiques par la personne concernée, services de santé, statistiques officielles, recherche médicale, « intérêt public » (strictement encadré).

Le reste peut être soumis à un régime de déclaration.

Principe de finalité

Art. 6, 2°

On collecte des données personnelles en vue d'une **finalité** déterminée (et pas « au cas où »).

On ne peut pas utiliser les données de manière incompatible avec la finalité initialement prévue.

Principe de légitimité

Art. 6, 2°

La finalité déclarée doit être **légitime**.

Voir le rôle du responsable de traitement vis-à-vis de la personne concernée : est-ce une finalité légitime pour une société de transports en commun de mettre en place des traitements de données visant à la gestion d'une régie publicitaire ?

Principe de proportionnalité

Art. 6, 3°

La collecte doit être **proportionnée** (nature et quantité des données) à la finalité.

Données « adéquates, pertinentes et non excessives », + objectives et licites.

Adéquation de la durée de conservation (5°)

Pour des contre-exemples, voir 95 % des formulaires web...

Formalités préalables

Les différents régimes

- **Déclaration (normale ou simplifiée) :** cas général (pas de données sensibles) ;
- **Dispense de déclaration :** certains traitements particuliers (« sans risques ») visés par la CNIL ou par la loi, présence d'un CIL dans l'organisation ;
- **Autorisation ou avis :** traitements portant sur des données sensibles.

Droits des personnes concernées

- Droit d'être informé (art. 32) ;
- Droit d'opposition (art. 38) ;
- Droit d'accès (art. 39) ;
- Droit de rectification, de suppression (art. 40).

Sécurité et conservation des données

Obligation de sécurité

Les données appartiennent toujours à la personne concernée (encore que...), mais le responsable de traitement a une obligation d'assurer « la sécurité des traitements et des données » et d'empêcher qu'elles soient « déformées, endommagées, ou que des tiers non autorisés y aient accès ».

Destruction des données

À la fin de la période de conservation, le responsable du traitement doit **détruire** les données, ou les « anonymiser » (illusoire, voir suite de la formation).

Commission Nationale de l'Informatique et des Libertés

Première autorité administrative indépendante en France (même type de statut que la Hadopi).

Créée par la loi de 78, compétences modifiées par la loi de 2004.

Membre français du G29.

Mission d'**information** et de **contrôle**.

`http://www.cnil.fr/`, nombreuses ressources en ligne

Encadrement des formalités préalables

La CNIL...

- Est destinataire des déclarations normales et simplifiées ;
- Délivre les autorisations pour les traitements portant sur des données sensibles ;
- Émet des avis sur les traitements mis en œuvre par arrêté ministériel, par décret en Conseil d'État ou par certains organismes en situation de service public ;
- Répond aux demandes d'accès indirect ;
- Peut délivrer des « labels ».

La CNIL doit être consultée sur tout projet de loi ou de décret concernant son périmètre juridique et peut faire des propositions législatives ou réglementaires.

Mission de contrôle-sanction

La CNIL...

- Organise des contrôles spontanés auprès des responsables de traitements ;
- Reçoit les « réclamations, pétitions et plaintes » et éventuellement y donne suite ;
- En cas de saisine ou de constatation d'une infraction, la CNIL peut :
  - Classer sans suite ;
  - Organiser une médiation ;
  - Procéder à un contrôle ;
  - Émettre un avertissement, une mise en demeure, une injonction de cesser le traitement, un retrait d'autorisation ;
  - Infliger elle-même une sanction (jusqu'à 150 000 €, puis 300 000 € plafonnés à 5 % du CA en cas de récidive).

La CNIL doit informer le procureur de la République des infractions dont elle a connaissance.

Le CIL : Correspondant Informatique et Libertés

Interlocuteur privilégié de la CNIL, nommé dans une organisation (publique ou privée).
Sa présence dispense l'organisation des déclarations (un registre est tenu en interne), pas des demandes d'autorisation.
Le CIL :

- Répertorie les traitements et s'assure qu'ils sont conformes à la loi ;
- Assure l'accès au registre ;
- Dispose d'un contact privilégié à la CNIL, ainsi que d'un réseau ;
- Établit un bilan annuel d'activité, tenu à disposition de la CNIL ;
- A une mission d'assurance qualité, de conseil, de vigilance.

Les critères techniques

Common Criteria for Information Technology Security Evaluation

Norme ISO/IEC 15408, successeur de l'*Orange Book* du DoD.
Section 7 : protection de la vie privée.

Exigences techniques pour assurer la vie privée

- **Anonymat** (*anonymity*) : incapacité des observateurs à déterminer l'identité d'un utilisateur ;
- **Pseudonymat** (*pseudonymity*) : idem, mais en imposant à l'utilisateur de répondre de ses actions ;
- **Non-chaînabilité** (*unlinkability*) : incapacité des observateurs à déterminer si deux actions ont été réalisées par le même utilisateur ;
- **Non-observabilité** (*unobservability*) : incapacité des observateurs à déterminer si une action est en cours.

Principes de conception

Souveraineté des données

Faire en sorte que **l'utilisateur conserve le contrôle** sur les données personnelles le concernant :

- Stocker en priorité données et/ou clés sur ses terminaux personnels ;
- Contrôler étroitement usage et diffusion, en imposant des obligations (obligations de sécurité, notifications, suppression...).

Principes de conception

Minimisation des données

cf. principe de proportionnalité

- Ne collecter que les données absolument nécessaires à la finalité ;
- Ne les transmettre/conserver que si c'est absolument nécessaire ;
- Détruire dès que possible les données non absolument nécessaires ;

Le tout dans les limites des obligations d'auditabilité des systèmes.

Le *Privacy by Design*

Principe

La protection de la vie privée, comme la sécurité, ne peut être efficace que si elle est pensée dès la conception du système. Les ajouts postérieurs ne peuvent pas espérer colmater des brèches de conception.

Le principe, de plus en plus mentionné dans les textes, doit concerner à la fois les intervenants techniques et non techniques, conjointement.

Exemples de mise en œuvre :

- Travail de spécification incluant experts techniques, juristes et décideurs ;
- Application de méthodes formelles de conception ;
- *Privacy impact assessments* ;
- Systèmes contraints par les politiques ;
- ...

Le *Privacy by Design*

Les sept principes du PbD

- Proactif plutôt que réactif, préventif plutôt que correctif ;
- Considérer la protection de la vie privée comme le réglage par défaut (*Privacy by default*) ;
- Intégrer la protection de la vie privée dans la conception du système ;
- Assurer des fonctionnalités complètes : viser une somme positive, pas une somme nulle ;
- Assurer la sécurité de bout en bout, avec une protection tout au long du cycle de vie ;
- Visibilité et transparence – viser l'ouverture ;
- Montrer du respect pour la vie privée des utilisateurs – centrer les systèmes sur les utilisateurs.

Cas d'étude : Facebook

Le risque majeur sur Facebook, c'est vous !

Les utilisateurs divulguent *volontairement* des données personnelles, parfois particulièrement sensibles.

. . . mais pas que !

- Le système proposé par Facebook peut favoriser les divulgations inconsidérées ;
- Le système d'applications peut s'avérer très invasif.

Cas d'étude : Facebook

Les risques liés à Facebook

- Risques de **sécurité** : usurpation d'identité, hameçonnage, prédation, chantage, arnaques diverses ;
- Risques de **profilage** : collection de données par les applications ou par Facebook, revente de listes de contacts et de données sociales ;
- Risques liés à l'**e-reputation** : exploration du réseau par les recruteurs, les employeurs, les clients...

Cas d'étude : Facebook

Cas d'école : Kevin Colvin, 2007

Stagiaire dans une banque britannique en 2007, probablement la première personne limogée à cause de Facebook, affaire très médiatisée.

Une photo de soirée postée sur FB a servi à prouver qu'il avait menti sur une absence pour urgence familiale.

Nathalie Blanchard, 2009

En arrêt maladie pour dépression grave, on lui retire ses allocations parce qu'elle poste une photo d'elle souriante dans un bar.

De nombreuses personnes se plaignent que des photos d'elles diffusées sur des réseaux sociaux ont un impact négatif sur leur employabilité.

Cas d'étude : Facebook

L'affaire du Tigre

Un magazine français indépendant, le Tigre, reconstitue la vie d'un utilisateur Facebook dans les détails, sans formellement révéler son identité, pour illustrer les dangers liés à la divulgation d'informations sur les réseaux sociaux.

Simples illustrations de la tendance psychologique identifiée par Westin dans son article *"Freebies" and Privacy : what net users think*.

Cas d'étude : Facebook

Quelle responsabilité pour Facebook ?

- La *Privacy Policy* (5830 mots) est plus longue que la constitution des États-Unis ;
- 50 réglages relatifs à la vie privée, plus de 170 options ;
- Modification des *terms of service* parfois inconsidérés.

(chiffres Mai 2010)

Conséquence : La plupart des utilisateurs ne prennent pas la peine de faire ces réglages ni de se poser les questions (complexes !) correspondantes.

Cas d'étude : Facebook

Les applications, sources de risques

- Les conditions d'accès et de partage des données personnelles par les applications sont souvent outrancières (profilage comportemental) ;
- La plupart des applications exigent l'abandon de la connexion chiffrée (SSL/TLS) ;
- De nombreuses applications organisent le « spam » des pages Facebook (notamment en piégeant les utilisateurs en les forçant à « aimer » un contenu sans qu'ils en soient conscients) ;
- Ce spam cache souvent une tentative d'escroquerie (conditionnant l'accès à une vidéo, par exemple, ou à « qui visite votre profil »), qui peut dans le pire des cas déboucher sur un paiement bancaire ou une infection informatique.

Cas d'étude : Facebook

Les questions à se poser

- Quels sont les différents cercles de connaissances, en terme d'intimité, que je souhaite gérer ? cf Alten
- Lorsque je publie quelque chose, qui peut le voir ? Est-ce ce que je souhaite ?
- Est-ce que je devrais supprimer les informations que j'ai postées dans le passé ?
- En cas de problème technique ou de divulgation par un tiers, est-ce que telle ou telle information publiée pourrait me porter préjudice ?
- **Est-ce légitime pour moi de publier cela ?** Est-ce que mes contacts souhaitent connaître ces aspects de ma vie privée ?
- Le développeur de telle application a-t-il besoin d'avoir accès à mon profil, à mes contacts, à mes photos... ?

Facebook *vs* Europe

L'affaire Max Schrems

Étudiant en droit autrichien, il faut valoir auprès de Facebook son droit d'accès aux données le concernant (en vertu du droit irlandais).

Il reçoit un CD correspondant à une liasse de 1200 pages.

Après une analyse minutieuse des données, il dépose 22 plaintes contre Facebook auprès du *Data Protection Commissioner* irlandais.

Détails de l'affaire, en cours :

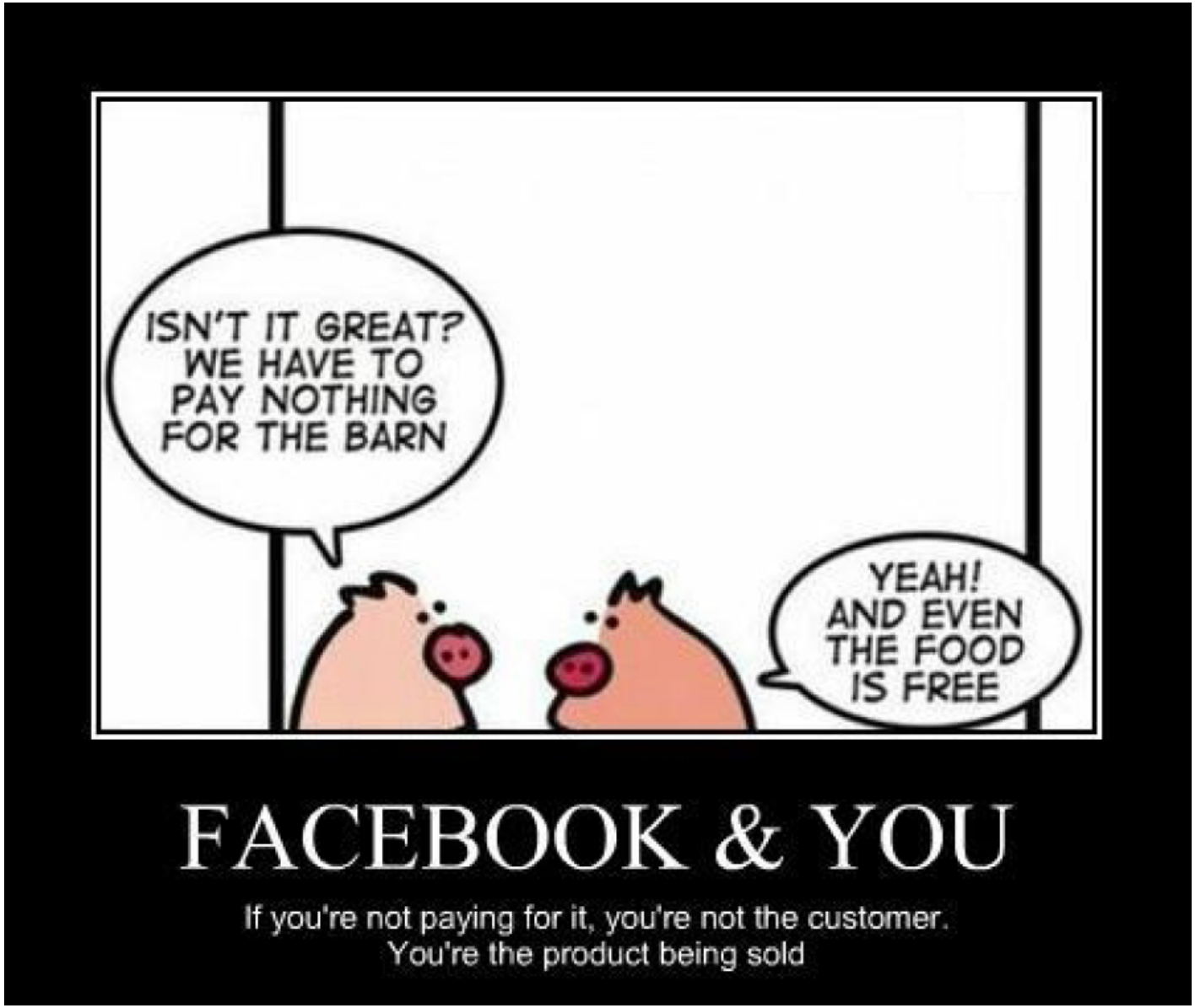
`http://www.europe-v-facebook.org/`

Facebook *vs* Europe

L'affaire Max Schrems : quelques motifs de plaintes

- Les « pokes », les messages postés et les messages privés sont conservés même après leur suppression par l'utilisateur ;
- Facebook collecte des informations sur des non-utilisateurs pour créer des profils de remplacement ;
- Les informations collectées via le *friend finder* sont utilisées sans le consentement de l'utilisateur ;
- Les utilisateurs ne connaissent pas les paramètres de re-publication des messages postés sur les pages d'autres personnes ;
- La demande d'accès n'a pas reçu une réponse suffisamment complète ;
- ...

Facebook : le modèle « gratuit »



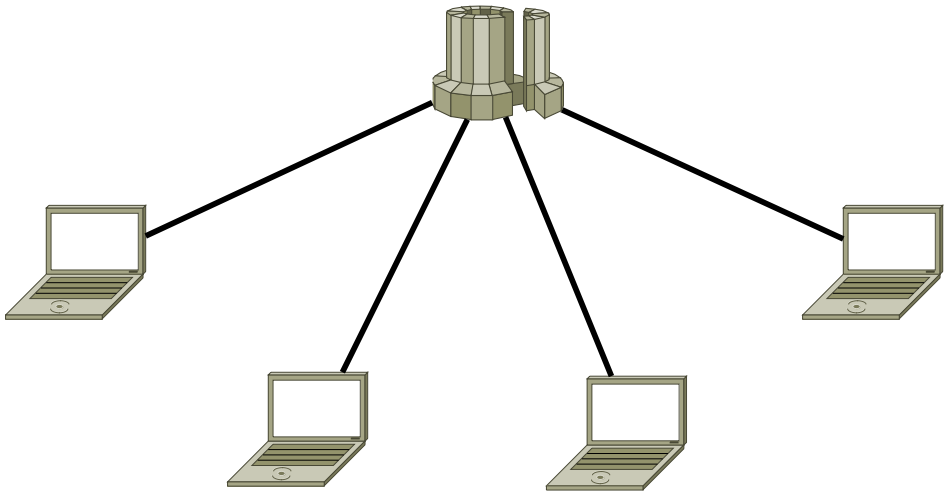
Alternatives à Facebook ?

Architectures centralisées

Exemples nombreux : Facebook, LinkedIn, Twitter, FourSquare...

Relative facilité de conception, de déploiement, d'administration...

Une autorité centralisée peut exercer un contrôle unilatéral sur les informations des usagers.



Alternatives à Facebook ?

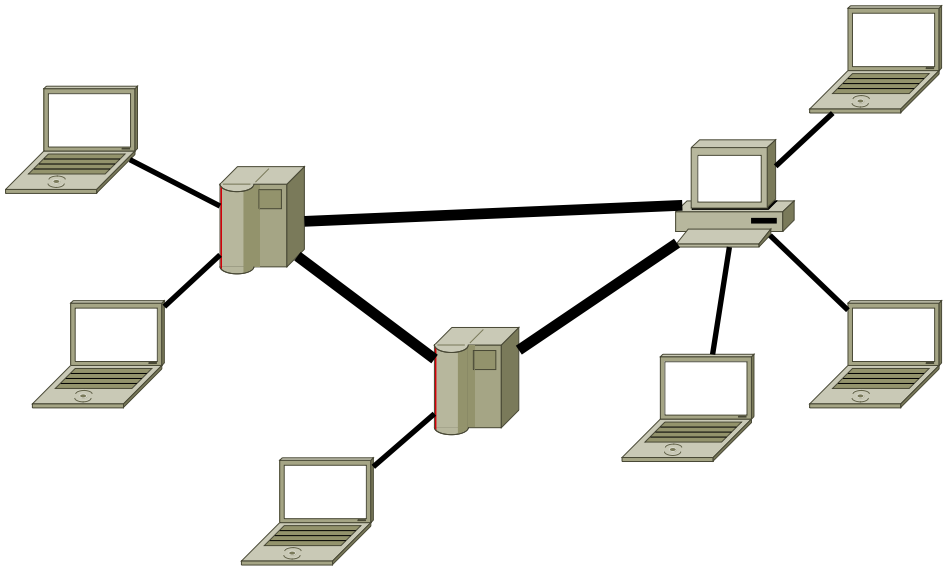
Architectures décentralisées

Diaspora*, SuperNova, PeerSon...

Les utilisateurs se connectent à un *superpeer* de leur choix, qui leur fournit une partie des services.

Répartition de la charge de calcul, tout en permettant aux utilisateurs de rester des « clients », possibilité d'avoir une gestion collégiale...

Les *superpeers* restent un point de centralisation du contrôle et peuvent être sensibles aux collusions.



Alternatives à Facebook ?

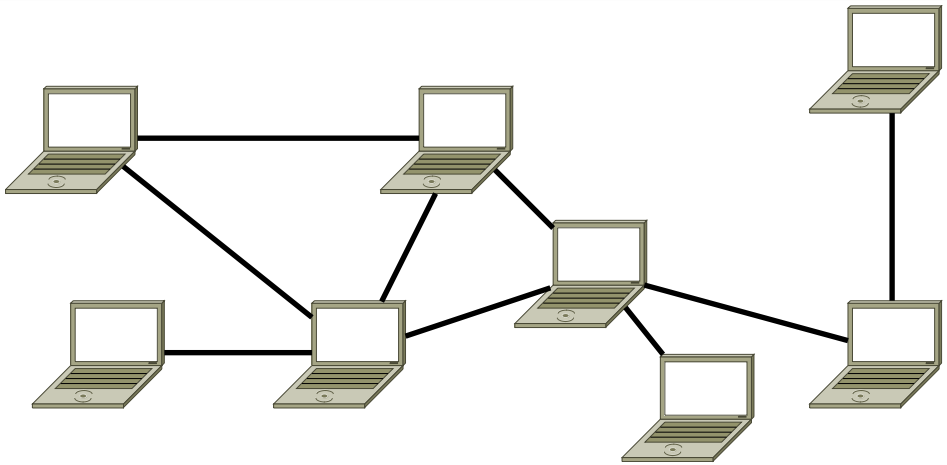
Architectures complètement distribuées

PrivacyWatch, Safebook, FOAF...

Tous les pairs sont « égaux » et responsables d'une partie des services fournis par le système.

Aucune entité ne dispose de plus de pouvoir ou de contrôle (pas de point de faiblesse désigné), potentiellement meilleur contrôle des utilisateurs sur leurs données.

Problèmes de disponibilité des données et d'application des politiques complexes.



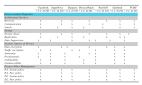
Alternatives à Facebook ?

	Facebook					SuperNova					Diaspora					PrivacyWatch					PeerSoN					Safebook					FOAF				
	?	*0*	*C*	*D*	*FD*	*?*	*0*	*C*	*D*	*FD*	*?*	*0*	*C*	*D*	*FD*	*?*	*0*	*C*	*D*	*FD*	*?*	*0*	*C*	*D*	*FD*	*?*	*0*	*C*	*D*	*FD*	*?*	*0*	*C*	*D*	*FD*
Privacy-related Properties																																			
Architectural Services																																			
Retrieval			x					x					x					x					x					x					x		
Communication			x					x					x					x					x					x					x		
Search			x				x						x				x						x					x					x		
Storage																																			
Storage Space			x					x					x					x					x					x				x			
Replication			x				x						x				x						x					x							
Data Suppression		x			x								x					x				x							x						
Security Aspects of Privacy																																			
Data encryption		x						x				x						x					x				x								
Traffic encryption			x		x								x				x						x					x							
Anonymity		x			x					x								x					x					x							
Pseudonymity		x			x					x							x						x					x							
Unlinkability			x		x					x								x					x					x							
Unobservability			x		x					x								x					x					x							
Privacy Policy Management																																			
P.A. System policy			x					x					x					x					x					x					x		
P.A. Peer policy			x					x					x					x					x					x					x		
P.E. System policy			x					x					x					x					x					x					x		
P.E. Peer policy			x					x					x					x					x					x					x		

Crédits iconographiques

Facebook, Inc. (`http://www.facebook.com/`)

Geek & Poke, *The "Free" Model* (`http://geekandpoke.typepad.com/geekandpoke/2010/12/the-free-model.html`), PBH3, *Facebook & You* (`http://twentytwowords.com/2011/09/22/facebook-and-you-if-youre-not-paying-youre-not-a-customer/`)



R. Paiva Melo Marin, G. Piolle & C. Bidan, *An analysis grid for privacy-related properties of social network systems*, in Proceedings of the ASE/IEEE International Conference on Social Computing, pp. 520–525, IEEE Computer Society publisher, Washington D.C., USA, 2013