Keynote Speech: Sylvia Johnigk (Vorstand Forum InformatikerInnen für Frieden und gesells. Verantwortung e.V.)

Wir müssen Freiheitsarchitektinnen werden

Anleitung für Männer: Das ist eine Keynote, die ich auf der Informatica Feminale gehalten habe, auch wenn ich deshalb ausschliesslich die weibliche Form gewählt habe, seid ihr mit angesprochen. Ihr werdet es verkraften./tragt es wie ein Mann ;-)

Als ich gefragt wurde, ob ich eine Keynote zu dem Thema “Datenschutz nach den Enthüllungen durch Edward Snowden” halten könne, dachte ich mir: Klar - da gibt es vieles was ich dazu sagen kann, aber dann dachte ich mir: was helfen schon schöne, schlaue Reden, wenn danach alles so weiter geht, wenn sich nichts ändert, weil Sie die Zuhörerinnen nicht wissen, was sie tun können oder weil ich Sie nicht davon überzeugen kann, dass wir etwas tun müssen und es sogar können, wenn wir nur wollen.

Edward Snowden hat uns klar gemacht, dass Geheimdienste egal welcher Coulor, in einem vorher nicht vorstellbaren Umfang, unsere Verfassung und unsere Grundrechte mit Füßen treten. Galt ich bislang im Freundeskreis als paranoid, weiss ich jetzt: ich war nicht paranoid genug!

Snowden hat enthüllt: Wir haben es mit massenhafter Überwachung unserer Metadaten zu tun. Das sind Verbindungsdaten, die Informationen preisgeben wie: Wer hat wann, mit wem Emails geschrieben, wer hat wann mit wem telefoniert, oder wer hat wann, welche Internetseiten besucht. Zusätzlich geht es, um die gezielte Überwachung von Millionen Erdenbürgern, den angeblichen Terroristen bzw. Terrorverdächtigen.
Terrorverdächtige verlieren ihre Menschenrechte – aufgrund eines Verdachts. Kann man sie trotzdem in Foltergefängnisse wegsperren ohne, dass sie jemals ein Recht auf einen fairen Prozess haben? Darf man sie foltern, Waterboarden, stundenlang,

tagelang mit lauter Musik beschallen und grellen Licht bestrahlen, auf dem nackten Boden schlafen lassen, in kalten nassen Räumen unterbringen oder ohne Schatten im Freien? Alles ohne eine Chance auf Verteidigung? Ohne einem fairen offenen Prozesss. Lebenslang verdächtig weggesperrt?
In den letzten fünf Jahren wurden 1,5 Millionen Menschen neu in die Terrormerkliste der USA aufgenommen .
Terrorverdächtig kann jeder von uns werden - auf Grund von achso sorgsamen und unbestechlichen Algorithmen. Geheimen Algorithmen von Menschenhand geschrieben. Algorithmen treffen erst eine Vorauswahl aus Metadaten. Wer aufgrund seiner Metadaten auffällt, bei dem werden Inhaltsdaten abgeschnorchelt. Dazu gehören die Inhalte von Emails, SMS, Telefonaten, Chats, oder unsere Fotos und unsere Dateien auf dem Laptop, Daten von unseren Smartphones, was wir im Internet posten, und unsere Passworte, die wir für unsere Sozialen Netzwerke, Banking und Einkaufsativitäten nutzen. Wieder sind es Algorithmen, die die Daten auswerten. Auch diese Algorithmen sind geheim und treffen eine weitere Vorauswahl. Und ganz zum Schluss kommen - “irgendwelche” Geheimdienstler - nach irgendwelchen nicht kontrollierbaren Verfahren - zum Schluss: Du bist ein Terrorverdächtiger. Und dann sind Deine Menschenrechte futsch, weil du in deren Augen keine Menschenrechte verdient hast.
Wie meinte vor ca. einem Jahr ein amerikanischer Journalist in einer Talkshow? Er traue Algorithmen mehr als Menschen. Hat dem eigentlich irgendwer mit IT Knowhow schonmal gesteckt**,** dass die so vertrauenswürdigen Algorithmen von Menschenhand stammen? - Wohl kaum!

Aber ich glaube sogar, dass dies kein Einzelfall ist, sondern dass es leider viele Menschen gibt, die an die Unfehlbarkeit von Algorithmen glauben. Ein wirklich fataler Irrglaube. Dieser Irrglaube wird dadurch gesteigert, dass diese Algorithmen einer strengen Geheimhaltung unterliegen. Sie werden nicht in einem offenen wissenschaftlichen Diskurs überprüft. Und diese Algorithmen entscheiden darüber**,** wer Menschenrechte hat und wer keine Menschenrechte hat. Wir lassen uns von

Menschen, von Geheimdienstmitarbeitern mittels nicht überprüfbarer Algorithmen und Verfahren die Menschenrechte absprechen.

Nur sieht weder das Grundgesetz, noch die Verfassung der EU und auch nicht die internationale Menschenrechtscharta eine Unterscheidung in Menschen *mit* Menschenrechten und “terrorverdächtige” Menschen *ohne* Menschenrechte vor. Es gibt nur Menchen mit Menschenrechten, ohne - wenn - und - aber. Menschenrechte darf man als Mensch nicht verlieren können!
Glücklicherweise sieht dies der Europäische Gerichtshof für Menschenrechte in Straßburg genauso und hat Polen vor einigen Wochen wegen Menschenrechtsverletzung, genauer wegen der Duldung bzw. Unterstützung von US Foltergefängnissen auf polnischen Boden verurteilt. Die CIA hat in Deutschland mit Hilfe des Unternehmens CSC den deutschen Staatsbürger al Masri in ein Foltergefängnis verschleppen lassen. Nachdem bekannt wurde, dass einige Regierungsmitglieder darüber informiert waren, gerieten diese in Kritik. Wegen des Drucks von Außen und der erwiesenen Unschuld kam er nach mehreren Monate wieder frei.

Datenschutz ist ein Grundrecht, abgeleitet aus dem Recht zur freien Entfaltung der Persönlichkeit und der Menschenwürde, die der Staat zu schützen hat. Datenschutz soll Personen, deren Daten erhoben werden gegen Missbrauch schützen. Datenschutzgesetze sollen uns davor schützen, dass unsere Daten heimlich oder für andere fremdbestimmte Zwecke genutzt werden. Datenschutzgesetzte schränken - den Umfang und - den Anlass - aus dem Daten erhoben werden dürfen - auf das für den Zweck notwendige ein.

Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme dient dem Schutz von persönlichen Daten , die in informationstechnischen Systemen gespeichert oder verarbeitet werden. Dieses Recht wird im Grundgesetz zwar nicht explizit genannt. Es wurde allerdings 2008 durch das

Bundesverfassungsgericht als spezielle Ausprägung des allgemeinen Persönlichkeitsrechts (Art. 1 Abs. 1 GG , Art. 2 Abs. 1 i.V.m.) aus den vorhandenen Grundrechtsbestimmungen abgeleitet.
Vertraulichkeit und Integrität und somit die Verschlüsselung von Daten ist ein Grundrecht.

Alle diejenigen, die ihre Daten auf dem Laptop, Smartphone, Tablet oder ihre Email verschlüsseln **wenden** ihre Grundrechte an. Ebenso diejenigen, die Anonymisisierungstools benutzen, um sowohl Verbindungsdaten wie auch Inhaltsdaten zu verschlüsseln. Sie tun etwas - was völlig natürlich ist, sie schützen ihre Privatsphäre.
Nach dem Urteil des Bundesverfassungsgerichts ist die heimliche Infiltration informationstechnischer Systeme zum Zweck der Ausspähung nur dann zulässig, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen, dieses kann nur durch einen richterlichen Beschluss herbei geführt werden.
Mit diesem Urteil sollte klar sein, dass das massenhafte, anlasslose Auspähen in vielerei Hinsicht einen massiven Bruch der Grundrechte in Deutschland darstellt, der mit nichts zu rechtfertigen ist.
Die gezielte Infiltration von IT-Systeme, das heimliche Einbauen von Zusatzfeatures in persönlichen IT-Systeme ohne richterlichen Beschluss ist ein massiver Eingriff in die Demokratie und stellt einen tiefen Eingriff in die Privatsphäre der betroffenen Personen dar. Alle diejenigen, die überwacht werden sind Opfer von Algorithmen und Menschen, die solche IT Systeme erstellen oder bedienen.

Gerechtfertigt wird das alles mit der Bekämpfung des Terrorismus.
Ein gut ausgebildeter Terrorist wird sich von der Überwachung niemals schrecken lassen, er braucht für seine Anschläge weder unmittelbar das Internet noch ein Telefon. Er weiß, dass er überwacht wird und wird sich zu schützen wissen, wenn er nicht völlig blöde ist. Schlecht ausgebildete Terroristen werden vielleicht in Staaten

wie Iran, Irak, Nigeria, Syrien im Namen des Heiligen Krieges sich selbst auf einem Marktplatz oder in einer Schule in die Luft sprengen – weil sie es nicht besser wissen. Trotzdem oder gerade deshalb ist die anlasslosse Massenüberwachung keine Antwort. Terrorismus lässt sich so nicht bekämpfen. Stattdessen wird sich die Überwachungsspirale immer enger drehen, bis wir uns zu Tode überwachen. Der Anlass warum neben dem massenhaften abschnorcheln von Verbindungsdaten auch Inhaltsdaten abgeschnorchelt werden, wird immer geringfügiger werden. Hat man fast alle vermeintlichen Terroristen, kommen die Pädophilen, dann die Hooligans, dann Großkriminellen, schliesslich Kleinkriminelle und zum Schluss reicht vielleicht schon der Verdacht einer möglichen Ordnungswidrigkeit aus, um heimlich ohne richterlichen Beschluss einen Trojaner auf einem persönlichen Gerät zu installieren. Man muss nur in das Strafgesetzbuch schauen, dort gibt es seit 9/11 einen erkennbaren Trend, dass immer geringfügigere Straftatbestände ausreichen, um massive Einschnitte wie das Abhören von Telekommunikation zu rechtfertigen. Und auch das Strafgesetzbuch setzt Strafverfolgungsbehörden in ihren Massnahmen Schranken – ganz im Geiste des Grundgesetzes.

Zudem war in den letzten Jahren in Europa und den USA die Gefahr, Opfer eines Terroranschlags zu werden sehr gering. Und *dies* schließt bereits die Anschläge geistig verwirrter Menschen oder schießwütiger Amokläufer ein. Die Einzelfälle sind natürlich tragisch für die Opfer, wenn diese verletzt oder zu Tode kommen und es ist natürlich insbesondere tragisch für deren Angehörige. Bloss bislang sterben ein Vielfaches an Menschen bei Verkehrsunfällen, an Grippe, Krebs oder Malaria, etc. Wollen wir das Autofahren verbieten – völlig absurd oder? Wollen wir die Menschen zwingen sich gegen Grippe zu impfen zu lassen? Die ganze Überwachung kostet viel Geld, das man wesentlich sinnvoller nutzen könnte.

Terrorismus war und ist eine Gefahr, sie sollte aber nicht unser Leben bestimmen und schon gar nicht in der Wahrnehmung als schlimmeres Ereignis gelten als die Gefahr, Opfer eines Verkehrsunfall zu werden, oder der Angst an Grippe oder Krebs zu sterben, was wahrscheinlicher ist, als Opfer eines Terroranschlags zu werden.

Mir persönlich ist es relativ egal, ob ich Opfer eines Verkehrsunfalls werde, wo mich

ein Autofahrer erwischt, der sein Unglück in Alkohol ertränkt hat oder ob ich Opfer eines Terroranschlags werde, weil jemand für seine Ideale (wie absurd ich sie auch finde) tötet und mich dabei erwischt. Ich möchte weder das Autofahren verbieten, noch irgendwelche Religionen oder Ideale. Aufklärung und Bildung kann in beiden Fällen helfen, massenhafte Überwachung und Kontrolle dagegen nur gegen einem hohen Preis, nämlich der Aufgabe von Freiheiten und Grundrechten.

Ein demokratischer Staat, der aus Angst vor einigen wenigen seiner Bürgerinnen alle überwacht, allen misstraut ist krank.
Die Demokratie steht auf dem Spiel und die Frage sei erlaubt: leben wir überhaupt noch in einer Demokratie, oder erleben gerade den Anfang einer Epoche zurück in die Unfreiheit und Unterdrückung.
In den letzten Jahrhunderten kämpften in ganz Europa und den USA Besitzlose und Frauen für das Recht wählen zu dürfen und träumten von einer besseren, freieren Welt. In Deutschland durften erst Januar 1919 Frauen erstmals auf nationaler Ebene an Wahlen teilnehmen.
Während des Dritten Reichs gab es defacto keine Wahlen, da es nur eine Partei gab, andere waren verboten. Warum wohl?
In der DDR gab es die Einheitspartei SED mit den Blockparteien und somit ebenfalls keine Wahlmöglichkeit. Die Stasi hat alles und jeden in der DDR ausgespäht. Es gibt aus Sicht der Informatik allerdings einen wichtigen Unterschied zur aktuellen Überwachungstechnik. Das Archiv, in dem die ausgespähten Daten lagen, war ein Papierarchiv, dass vom Umfang her eher überschaubar war und in wenigen Gebäuden in der Nommanenstraße untergebracht war. Das System hat leider trotzdem jahrzehntelang funktioniert und während der Zeit viele Menschen unterdrückt und unbequeme Menschen weggesperrt, gefoltert oder in scheinbarer Freiheit schikaniert.
Permantente Überwachung bewirkt eine Bewußtsens- und Verhaltensänderung bei den Überwachten hin zum Konformismus.
Von beiden Diktaturen haben wir uns in Deutschland befreit bzw. wir sind befreit worden und wir sind es unseren Vorfahrinnen schuldig, dass wir die erkämpfte

Freiheit und Demokratie verteidigen und uns nicht aus den Händen reißen lassen, bloß weil unsere Regierung uns drohende Terroranschläge ankündigt, die nur durch die Massenüberwachung im Griff gehalten werden kann.
Dass nur knapp 25 Jahre nach dem Ende der letzten Diktatur und dem Überwachungswahn der DDR, Überwachung wieder salonfähig ist, ist um so bemerkenswerter, als dass dies ausgerechnet von einer Kanzlerin als Regierungschefin verantwortet wird, die selbst Jahrzehnte in einem Überwachungsstaat gelebt hat.
Wer Überwachung befürwortet, vergisst, dass freie Wahlen nur möglich sind, wenn die Bürgerinnen sich frei und unbeobachtet über die politische Lage informieren können, - wenn es keine Zensur gibt oder die Informationen über die politische Lage unabhängig, freizugänglich und vielfältig angeboten werden können. Das ist unter den Umständen ständiger Überwachung, Zensur und eingeschränkten Zugang zu Informationen nicht mehr möglich.
Das Grundgesetz wurde nach den schlimmen Erlebnissen des Dritten Reichs geschaffen, diese Gesetze sollten zukünftig und für alle Zeiten die Bürger und Bürgerinnen der Bundesrepublik Deutschland vor der Willkür des Staates schützen. Das Grundgesetz ist also das Schutzschild des Bürgers vor der Willkür des Staates. Im Grundgesetz kommt 23 mal das Wort Freiheit vor, jedes Mal im Zusammenhang mit den Rechten der Bürgerinnen und 5 Mal das Wort Sicherheit, jedes Mal im Zusammenhang mit den Pflichten des Staates. Da ist es bemerkenswert, dass ein Innenminister fabuliert, dass es ein Supergrundrecht Sicherheit gäbe.
Ein Supergrundrecht Sicherheit, dass über alle anderen Grundrechte steht, ist wie ein Elefant im Porzellanladen, der die Freiheit der Bürgerinnen mit den scheinbar schützenden Wesen des Staates zertritt.
Wie sagte Innenminister de Maiziere vor kurzem: wer das Internet nutzt gibt seine Grundrechte ab. Anscheinend ist im Internet wohl schon das Supergrundrecht Sicherheit implementiert. Es wird Zeit, dass wir dies rückgängig machen. Das Internet ist kein rechtsfreier Raum und schon gar kein grundrechtsfreier Raum.
Noch müssen wir leider auf Komfort und auf liebgewonnene Gewohnheiten

verzichten, wenn wir unsere Grundrechte verteidigen wollen.
Nichtsdestotrotz: Es ist an der Zeit für die digitale Selbstverteidigung.
Fangen wir an unsere Emails zu verschlüsseln! Wer, wenn nicht wir Informatikerinnen und an IT interessierte Menchen soll beginnen?
Wenn nur jeder Zehnte, vor allem hier in Deutschland seine Email verschlüsselt, machen wir es zwar nicht unmöglich die Inhalte unserer Nachrichten auszuspähen, aber wir machen es den Überwacherinnen schwerer. Sie brauchen mehr Ressourcen und müssen mehr Geld ausgeben oder sich auf wenige Einzelfälle konzentrieren.
Lernen wir, wie wir Emails verschlüsseln. Wenden wir es an, bis wir es können und geben unser Wissen weiter an Familienmitglieder, Freunde, Kommilitonen, Kollegen - an jeden, der es lernen will.
Sicher, Geheimdienste und alle die die Informationen sonst noch abfangen, wissen noch, wer mit wem kommuniziert, aber es ist ein Anfang. Wenn man den ersten Schritt getan hat, fallen die nächsten Schritte leichter. Verschlüsseln wir als nächstes die Daten auf den mobilen Endgeräten wie Laptop, Smartphone, USB Stick, etc.
Nutzen wir Anonymisierungstools wir Tor, wenngleich man dann in den USA und vielleicht auch anderswo schon als Extremist gilt. *Was* ist dieses Risiko hier in Deutschland für uns für ein Risiko, verglichen mit den *Risiken* die Menschen eingehen, die in China, im Iran, in Ägypten oder anderen Diktaturen leben und dort Tor nutzen. Diese Menschen riskieren ihr Leben, um für ein Gut zu kämpfen, dass wir noch haben: Freiheit und Demokratie. *W*enden wir unsere Grundrechte an, indem wir verschlüsseln oder Anonymisierungstools nutzen oder wollen wir uns einschüchtern lassen, aus Angst uns verdächtig zu machen? Aber was wollen die Geheimdienste und Befürworterinnen der Überwachung machen, wenn wir alle unsere Grundrechte anwenden und Emails verschlüsseln, beim Surfen wenigsten teilweise Tor benutzen? Nichts – sie können nicht viele Millionen von Menschen überwachen, die sich nicht überwachen lassen wollen und sich davor schützen.
In vielen Ländern ist Verschlüsselung nur möglich, wenn man einen Nachschlüssel beim Staat abgibt – zum Beispiel USA, Russland, Frankreich. Das ist ein Zustand, den wir in Deutschland verhindern müssen.

Es gibt noch viel mehr, was wir tun können.

Was den Geheimdiensten die Überwachung so leicht macht, ist die Art, wie wir Informatikerinnen Systeme designen.
Quellenoffene Software kann man unabhängig und transparent validieren und auditeren. Das es irgendwer auch tun muss, wurde schmerzlich bewusst durch den Heartbleed Bug, der in der OpenSSL Software versteckt war. Aber man (in diesem Fall waren es Mitarbeiter von Google) hat den Bug nur deshalb gefunden, weil sich endlich mal jemand die Arbeit gemacht hat, die Software zu untersuchen. Closed Source Systeme (Microsoft, Apple, Oracle, SAP, ..) können nicht unabhängig untersucht werden. Sie bieten den Geheimdiensten und Überwachungsbefürworterinnen jede Möglichkeit, Funktionen im Code zu verstecken, die direkt für die Überwachung genutzt werden können.
Wir können Systeme nach dem Prinzip Privacy by Design bauen. Warum muss es auch zukünftig so schwierig bleiben, Emails zu verschlüsseln oder die Daten auf den Endgeräten oder das Surfen im Internet zu anonymisieren? Privacy by Plug and Play, Privacy muss so einfach werden, wie es das Surfen selbst ist.
Wir können schon jetzt damit anfangen, unsere Autononmie zurück zu erlangen. Nutzen wir immer mehr Systeme, die zumindest quellenoffen sind: Ubuntu, OpenOffice auf Laptops, CyanogenMod auf unserem Smartphone.
Nutzen wir OpenstreetMap. Nutzen DuckDuckGo oder ixquick/start page als Suchmaschine.
Es gibt Browser Plugins, die erstmal alle Scripte sperren und somit verhindern das Tracker unser Surfverhalten erfassen, wie zum Beispiel No Script. Es gibt Enigmail, GnuPG, Tor, und ...
Noch besser: werden wir aktiver Teil der Community, bauen wir gemeinsam neue demokratische, transparente Systeme. Sämtliche Opensource Projekte freuen sich über Unterstützung, sei es monetäre Zuwendungen, sei es, dass man selber Module designt und programmiert.

Überlegen wir uns zukünftig vorher, ob wir unsere ganzen Daten einer zwar kostenfreien - aber ansonsten intransparenten Cloud anvertrauen wollen, ob wir Adressbücher zum Abgleich in Sozialen Netzwerken hochladen wollen, ob wir unbedingt die tausendste App auf unserem Smartphone laden müssen und dafür alle unsere Daten an den Provider übermitteln lassen, ihm Zugriff auf unseren Speicher überlassen, obwohl der Provider möglicherweise eine Kooperation mit den Geheimdiensten eingegangen ist.
Wir können nicht kontrollieren, was andere Menschen mit unseren Daten tun und so lange wir dies nicht können, müssen wir uns entscheiden, immer und immer wieder. Wollen wir die Freiheit haben, selbst zu bestimmen, wer unsere Daten nutzt und in welchem Umfang. Wollen wir wissen was der Provider mit unseren Daten macht, ob daraus ein Profil erstellt wird, wem er seine Erkenntnis weiter verkauft, oder ob er Teil des Überwachungsapperat ist und er einen Teil dazu beiträgt, ob wir Extremist, Terrorist, Mensch mit Menschenrechten oder ohne Menschenrechte sind.

Systeme sind nie wertfrei, aber wir können entscheiden, in welcher Gesellschaft wir leben wollen, welche Werte uns wichtig sind. Wir Informatikerinnen sind in der Lage Systeme zu bauen, die unsere Werte stützen und schützen.

Als Informatikerinnen können wir unsere Zukunft mitgestalten. Gestalten wir unsere Zukunft in Freiheit.