



NATIONAL NETWORK
TO END DOMESTIC
VIOLENCE

2001 S STREET NW
SUITE 400
WASHINGTON, DC 20009

www.nnedv.org

The National Network to End Domestic Violence (NNEDV) has serious concerns about the safety risks of RFID to victims of domestic violence, sexual assault, dating violence, and stalking.

NNEDV, a not-for-profit organization incorporated in the District of Columbia since 1995, is a network of state domestic violence coalitions, representing over 2,000 member organizations nationwide. NNEDV serves as the national voice of battered women and their children and those who provide direct services to them. From testifying before Congress on domestic violence issues to assisting state coalitions in better serving the needs of the victim, NNEDV is a national leader in efforts to assist battered women in protecting themselves and their children.

Domestic violence is a terrifying reality for women and children across the United States.¹ Sadly, domestic violence is quite prevalent, and women continue to be the vast majority of victims. Millions of women are physically abused by their husbands or partners each year.² In addition, the National Institute of Justice reported that 4.9 million intimate partner rapes and physical assaults are perpetrated against U.S. women each year.³

Domestic violence, sexual assault and stalking are the most personal of crimes, and the more personal information that the perpetrator has about his victim, the more dangerous and damaging the perpetrator can be. Unfortunately, leaving the relationship does not stop the violence. In fact, the most dangerous time for a victim of domestic violence is when she takes steps to leave the relationship.⁴ After a victim has managed to escape her abuser, disclosure of her identity and location can create life-threatening danger and life-changing stigma for victims. Many victims are stalked relentlessly for years after having escaped from their partners. Fifty-nine percent of female stalking victims are stalked by current or former intimate partners,⁵ and 76% of women killed by their abusers had been stalked prior to their murder.⁶ Batterers who stalk their former partners are the most dangerous and pose the highest lethality risk.⁷ The severity of this “separation violence” often compels

¹ Because the vast majority of victims of domestic violence and sexual assault are women, throughout these comments the National Network to End Domestic Violence (NNEDV) will use only female nouns and pronouns when referring to victims or survivors. See Callie Marie Rennison & Sarah Welchans, U.S. Department of Justice, *Intimate Partner Violence*, at 1 (2000) (estimates that 85% of reported assaults on partners or ex-partners are committed by men against women). NNEDV acknowledges that men are also victims of domestic violence, especially in same-sex relationships.

² See Patricia Tjaden & Nancy Thoennes, Nat'l. Inst. of Justice, *Prevalence, Incidence and Consequences of Violence Against Women: Findings from the National Violence Against Women Survey*, at 2, 7 (1998). See *ibid.* at 11. See also *United States v. Morrison*, 529 U.S. 598, 632 (2000) (Souter, J., dissenting) (citing estimates four million female assault victims every year).

³ Patricia Tjaden and Nancy Thoennes, National Institute of Justice and the Centers of Disease Control and Prevention, *Extent, Nature, and Consequences of Intimate Partner Violence* (2000); Dr. Callie Marie Rennison, Department of Justice, Bureau of Justice Statistics, *Intimate Partner Violence, 1993-2001* (February 2003).

⁴ Ronet Bachman and Linda Salzman, Bureau of Justice Statistics, *Violence Against Women: Estimates From the Redesigned Survey 1* (January 2000).

⁵ Tjaden & Thoennes. (1998) “Stalking in America,” Nat'l. Inst. of Justice.

⁶ McFarlane, et al. (1999). “Stalking and Intimate Partner Femicide,” *Homicide Studies*.

⁷ Barbara J. Hart, *Assessing Whether Batterers Will Kill*. (This document may be found online at: <http://www.mincava.umn.edu/hart/lethali.htm>). Jacqueline Campbell, *Prediction of Homicide of and by Battered Women*, reprinted in J. Campbell, ed. (1995) *Assessing Dangerousness: Violence by Sexual Offender, Batterers, and Sexual Abusers* 96.

women to stay in abusive relationships rather than risk greater injury to themselves or their children. Many of those who succeed in leaving their abuser live in constant fear of being found. This constant fear of being found is only exacerbated by the potential for a victim's abuser to obtain important information about the victim's location and activities through RFID databases.

Victims often take extraordinary and desperate steps to hide their location, sometimes even changing their identities to avoid being found by their abusers. Steps they take can include the following:

- Fleeting across the state or country to seek safety.
- Using post office boxes and unlisted phone numbers.
- Using only prepaid cell phones to avoid having a phone account tied to a home address.
- Changing names through the court system and sealing the name change record.
- Changing Social Security numbers through the Social Security Administration.
- Relocating to confidential and undisclosed shelter locations.
- Enrolling in state address and voter record confidentiality programs.
- Sealing identity and location information in court filings.

These extraordinary, difficult and often costly steps that victims of domestic violence, sexual assault and stalking take to shield their location and identity could be futile in light of proposed RFID implementations.

NNEDV Concerns and Questions

Any plan to begin using RFID in identification cards raises immediate questions for survivors of domestic violence and their advocates since this provides yet another way that her abuser can track, stalk and monitor her movement. The privacy implications of RFID are far reaching, as noted in an April 2007 report by the U.S. Department of Commerce, National Institute of Standards and Technology:

The RFID system does not have to store personal information to have privacy implications. For example, the tag on a bottle of prescription medicine may identify the drug in the bottle, but not the identity of the person for whom the prescription was written. Nonetheless, the individual taking the medicine may still perceive the possession of the drug as personal information if scanned and read by another, as it might reveal information about a medical condition that the individual considers private.

Similarly, the individual does not have to own a tagged item for the RFID system to have privacy implications. For example, if an employee carries an employer-tagged computer or tools, then RFID technology potentially could be used to track the employee's whereabouts. The employee may agree to be on-call after business hours but could consider his or her location during those times as personal information.⁸

⁸ Tom Karygiannis, et al. *Guidelines for Securing Radio Frequency Identification (RFID) Systems*. National Institute of Standards and Technology, US Dept of Commerce (April 2007). Available at: http://csrc.nist.gov/publications/nistpubs/800-98/SP800-98_RFID-2007.pdf.

What information will be captured each time an RFID tag is scanned? Where will the information be stored and for how long?

Many members of the public have heightened privacy needs, such as police officers; witnesses in dangerous crime cases; victims of all crimes including domestic violence, sexual assault, and stalking; all children; and many others. According to testimony by the Government Accountability Office, "Once a particular individual is identified through an RFID tag, personally identifiable information can be retrieved from any number of sources and then aggregated to develop a profile of the individual. Both tracking and profiling can compromise an individual's privacy."⁹

The crime of identity theft and other types of fraud will undoubtedly be fueled by easy access to personal identifiers and other personal information. However, there are far more serious consequences to merging disparate electronic files of personal information into massive databases. We are becoming a "dossier society." Extensive histories – whether accurate or not – are increasingly available at the click of the mouse to virtually anyone. Law professor Jeffrey Rosen discusses the negative consequences of a dossier society in his 2000 book, *The Unwanted Gaze: The Destruction of Privacy in America*. His main concern, as is ours, is the compilation of bits and pieces of information about survivors from disparate sources, taken out of context, are then used to form conclusions and make decisions about all people, including victims of domestic violence.

While adding RFID chips to government identification cards may only initially put a victim's location and identity at risk, the inevitable data mining that will occur will combine other information, already culled and combined, into large repositories. All too often, victims of domestic violence are discriminated against in applications for employment and housing and denied health insurance. It is not hard to imagine that an RFID chip inserted into an identification card could facilitate discrimination without a victim even knowing the RFID chip was scanned from a distance and used to find out personally identifying information.

How will this plan counter "skimming" and "eavesdropping"?

RFID tags are remotely and secretly readable. A person with an unauthorized RFID reader can read an individual chip without the chip's holder knowledge by simply "skimming" the information. In addition, someone can eavesdrop on by intercepting data as it is read by an authorized RFID reader. As companies continue to develop a variety of handheld RFID readers, it is not hard to imagine the day when RFID chip replaces the bar code on consumer products, thus generating the need for hundreds or thousands of RFID readers in the hands of employees around the nation. Furthermore, a reader can be quite far away and still skim or eavesdrop on information. While it was initially thought that RFID tags could only be read at a very close distance, tests have shown that RFID tags can be read from 70 feet or more, posing a significant risk of unauthorized access.¹⁰

In one case, a computer expert was able to clone a United Kingdom's electronic passport by using a commercially available RFID reader (which cost less than \$350) and software that took him only a few

⁹ Linda D. Koontz, Dir., Info. Mgmt. Issues, Gov't Accountability Office, *Testimony Before the Subcom. on Homeland Sec., H. Comm. on Appropriations*, 110th Cong. (Apr. 14, 2007). Available at <http://www.gao.gov/new.items/d07630t.pdf>.

¹⁰ See Ziv Kfir and Avishai Wool, *Picking Virtual Pockets using Relay Attacks on Contactless Smartcard Systems* (Feb. 22, 2005). Available at <http://eprint.iacr.org/2005/052>; Scott Bradner, "An RFID warning shot," *Network World*, Feb. 7, 2005.

days to write.¹¹ In assessing an RFID-enabled U.S. passport, one expert cloned the RFID tag and another used characteristics of the radio transmissions to identify individual chips; those researchers spent only a few weeks attacking the RFID-enabled passports.¹²

Victims often go to heroic and exhausting levels to avoid providing personally identifying information to a variety of entities, including, but not limited to, grocery stores (since they have to provide contact information to partake in discount programs), auto-mechanics (where they wait until their car is finished, rather than provide an address and phone number that will go into the company's database), and voter databases (many victims decide they cannot safely register to vote if the state does not allow them to provide a confidential or sealed voter address). Currently, a victim must worry about information she directly reveals, verbally or by displaying her identification (ID) card to another entity. If RFID chips are inserted into identification cards, a victim will need to also worry about even carrying her ID card with her, since the information on the RFID chip could be intercepted and her identity, location, and activities compromised – potentially putting her in life-threatening danger.

Will a massive, cross-referenced database be created, which will be able to track each and every time a RFID tag passes a reader?

A massive, cross-referenced database will enable abusers and stalkers to have more opportunities to track their victims. Abusers and stalkers commonly use social engineering and pretexting to track down their victims. These persistent and creative perpetrators do not reveal that they are hoping to harm their victims; rather they couch their query as concern for the victim's health or impersonate law enforcement or other authorized individual. Enormous databases containing victims' location information could truly be fatal.

While government entities may choose to limit their statewide and national databases (when REAL ID is implemented) to only the information currently contained on the face of a government identification card, private data mining companies will go to incredible lengths, through legal and often illegal means, to acquire this data; they will then combine the RFID chip information with additional mined data about all members of the community, including victims of domestic violence. Since private data mining companies already warehouse court records, retail purchases, and information about family members and neighbors, victims will unknowingly have their identity, location, and activities merged with other information about themselves. This would be invasive for all people, but dangerous for victims who are running for their lives.

Given the numerous accounts about people misusing their authorized access privileges, how will user logins and user privileges to this database be maintained? Who will have access to this information, and what screening process will be available to ensure that the information is not misused for identity theft or to locate a victim of domestic violence?

Given the incalculable number of people that will have access to this data, it will be possible for a stalker or abuser to obtain RFID records either as a user or employee or through someone who has legitimate access to these records. Given that most security breaches occur from internal and authorized users, limiting access to personally identifying information will minimize, but not eliminate inappropriate access.¹³

¹¹ Steve Boggan, "Special Report: Identity Cards: Cracked It!" *Guardian*, Nov. 17, 2006.

¹² Bruce Schneier, "The ID Chip You Don't Want in Your Passport," *Washington Post*, Sept. 16, 2006.

¹³ A *New York Times* story highlights multiple examples of unauthorized searches: (a) when Bill Clinton had surgery in 2004, (b) 1,500 attempts to see a local athlete, and (c) dozens of attempts to view the records of a victim of a

In September, a Homeland Security agent was indicted for accessing a Homeland Security database more than 160 times to track his former girlfriend.¹⁴ After a seven-month relationship, the woman tried to end it, and the agent “threatened numerous times that he would have her deported or will kill her and her family.” Between May 2003 and March 2004, he accessed the Treasury Enforcement Communications System (TECS) database at least 163 times to track the woman's movements. According to the U.S. Attorney’s Office, federal agents are authorized to use that database only in the performance of their official duties and not for personal reasons. Law enforcement agents receive training in TECS security and privacy and are issued unique passwords to access the database so their system use can be monitored.¹⁵ This example shows that it is possible for individuals to misuse authorized access to stalk their victims.

In another case of misuse of authorized access, an abuser was given information about a victim’s location by a police officer. The victim had a restraining order against her “horribly abusive ex-husband who had threatened her with a gun.”¹⁶ After their separation, he located her and threatened to burn down her house. The victim moved to a new town, got a new job and even remarried. Her ex-husband found her again after a police officer searched a Department of Motor Vehicles database and gave her ex-husband the information.

In small, rural communities, there are never “six degrees of separation” between a victim, an abuser, and the government employees with access to sensitive data. Friends and family members of abusers often work in offices with legitimate access. Often an abuser will tell a compelling tale about how worried he is about the victim, never explaining that in truth, he is trying to track down his ex-wife to kill her. Combining real-time tracking ability with identification documents will increase the risk to victims.

Will everyone registering for an identification card be notified about the RFID tag contained within it? How will notification be handled?

As noted by the Institute of Electrical and Electronics Engineers, “RFID systems should be built on the concept of openness and transparency. Companies and governments using or specifying the use of RFID technology should be required to include clear notices regarding what data are collected and how it will be used for its applications and implementations.”¹⁷ One of the challenges with collecting data is that once data is collected, researchers, policymakers, statisticians and others often clamor and beg for access to that data. Even if there is currently no intent to share data, combine data or develop a massive cross-referenced database, what will happen when this massive database comes into being in the future?

domestic homicide. Available at: www.nytimes.com/2006/12/03/business/yourmoney/03health.html?ex=1322802000&en=b2c0f7946b4e3d9d&ei=5090.

¹⁴ Sharon Gaudin, “Federal Agent Indicted For Using Homeland Security Database To Stalk Girlfriend,” Information Week, Sept 20, 2007. Available at: <http://www.informationweek.com/shared/printableArticle.jhtml?articleID=201807903>.

¹⁵ Ibid.

¹⁶ Kevin Murphy, “Officer’s Actions will Cost 25,000,” *GazettXtra*, Feb. 15, 2007. Available at <http://www.gazetteextra.com/mezera021507.asp>.

¹⁷ IEEE, “Developing National Policies on the Deployment of Radio Frequency Identification (RFID) Technology,” Feb 17, 2006. Available at: <http://www.library.ca.gov/crb/rfidap/docs/IEEE-RFIDPositionStatement.pdf>.

In addition to robust notice, will there be any way for people with heightened risk to “opt-out” from having an RFID chip in their ID card? Throughout other parts of society, victims and other protected parties, including elected officials and undercover agents, are able to seal records, change identities, and are afforded other additional safety protections. Given that the Social Security Administration allows victims in grave risk to change their identities, including their social security numbers, it would seem that a government program attempting to track people using a new technology should consider exempting people who are already at great risk.

Since all good technology initiatives include quality assurance and auditing processes, what methods will be used to ensure audit trails exist and are checked regularly?

Corporations and organizations should create a comprehensive and timely process for quality assurance PRIOR to beginning to install/use RFID tags. A neutral office should assist or oversee an audit process and initiate random sampling as ongoing quality control. Since it can be assumed that errors will occur, a timely remedy process should be developed prior to implementing an RFID system. Depending on the nature of the error, victim safety and citizen privacy could be compromised, and time is often of the essence. All staff with any level of access to the RFID tag or the item/card containing the tag should be required to participate in training. In addition, all staff should know what process to follow in cases of error or if a citizen or customer requests a restriction of access or a special restriction on their personal information.

Audit trails are most often used to investigate crimes that have already been committed. They do not prevent an abuser from misusing the information to hunt down their victim, but rather prove how the victim was located. For audit trails to prevent personal harm, government entities would need to create a “flagging system” that would flag the accounts of elected officials, undercover agents, and victims who are in the justice system so that when their records are queried, an immediate alert would be sent to a supervisor or internal affairs unit to investigate. Without a real-time flagging system, audit trails will not prevent a domestic violence homicide, but merely assist in the prosecution after the fact.

Conclusion

In conclusion, victims of domestic violence face an increased risk when data is collected, kept and breached. They risk much more than identity theft or other types of fraud. They risk their lives and the lives of their children. All companies, organizations and groups that collect and retain personal information about their customers should enhance the security and privacy options available to consumers and create levels of security that are not easily breached from within or from outside of the company. Given the creative and persistent tactics of criminals, abusers and stalkers, companies and governments must work with consumers and citizens to identify the methods of security that will work best for general consumers, as well as methods of security for consumers in higher risk situations, such as victims of domestic violence and other groups with heightened privacy needs. Unfortunately, adding RFID chips to identification cards could inadvertently provide a government-run stalking aid and put victims at more risk.¹⁸

¹⁸ For more information, please contact: Cindy Southworth, MSW, Director of the Safety Net Project at the National Network to End Domestic Violence. 202-543-5566, ext 117 or SafetyNet@nnev.org.